Mumbai B.Sc.IT Study

With Solved University Question Papers.

MU

Strictly as per the new revised syllabus of Mumbai University

INTERNET TECHNOLOGY

T. Y. B. Sc. (Information Technology)
Semester - VI

Mahesh Mali Chetana Khetmal

Tech-Max Publications, Pune
Innovation Throughout
Computer Science Division

Be sure with Vidyalankar
Since 1960

MIE21A Price ₹ 165/-

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Name Kamal Thakur

|| Shree Ganeshay Namh ||

INFOVISION INFOTECH

Private Batch at Dadar center by our reputed Techmax Book Authors

" Internet Technologies "

Fees : Rs.3000 only

Learn and Develop Your Final Year Projects

VB.NET and SQL SERVER 2008 (Desktop App) /
ASP.NET and SQL SERVER 2008 (Web App)

Early Bird Discount 5000 / Person

 # Unique Features #

We will guide for Project ideas and topic

We will teach you programming languages

We will help you in coding for developing your project

Improves your knowledge level

Makes employment ready

Contact for Admission : 09220877214 (Sachin) /
09821625805 (Sachin)

Location : Dadar

Kamal T Universe

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Internet Technology

Semester VI – B.Sc. (Information Technology)
(Mumbai University)

Strictly as per new revised syllabus

Prof. Mahesh Mali
M.E. (Computer Engineering)*
B.E. (Information Technology)
St. Francis Institute of technology, Borivli (W), Mumbai
I.T. Department

Prof. Chetana Khetmal
M.E. (Computer Engineering)*
B.E. (Information Technology)
K.C. College of Engineering, Thane (E)
I.T. Department

Tech-Max Publications, Pune
Innovation Throughout
Computer Science Division

MIE21A Price ₹ 165/-

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Internet Technology

Mahesh Mali, Chetana Khetmal
(Semester VI, B.Sc.(IT), Mumbai University)

Copyright © by Tech-Max Publications. All rights reserved. No part of this publication may be reproduced, copied, or stored in a retrieval system, distributed or transmitted in any form or by any means, including photocopy, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

This book is sold subject to the condition that it shall not, by the way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior written consent in any form of binding or cover other than which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above.

First Edition : January 2014

This edition is for sale in India, Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Sri Lanka and designated countries in South-East Asia. Sale and purchase of this book outside of these countries is unauthorized by the publisher.

Printed at : Image Offset, Dugane Ind. Area Survey No. 28/25,
Dhayari Near Pari Company, Pune – 41, Maharashtra State, India.
E-mail : rahulshahimage@gmail.com

ISBN 978-93-5077-421-2

Published by
Tech-Max Publications
Head Office : B/5, First floor, Maniratna Complex, Taware Colony,
Aranyeshwar Corner, Pune - 411 009. Maharashtra State, India
Ph : 91-20-24225065, 91-20-24217965. Fax 020-24228978.
Email : info@techmaxbooks.com,
Website : www.techmaxbooks.com

Branch Office : Ground Floor, A-133, Okhla Phase-II, New Delhi - 110020

(Book Code : MIE21A)

Price ₹ 165/-

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Dedicated to ...

My Dear
Wife
Kasturi Mali

- Mahesh Mali

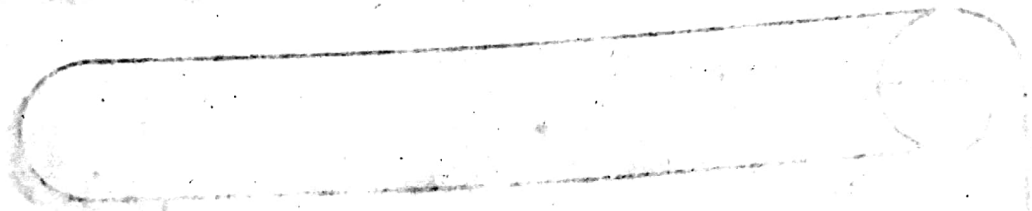
And ...

My Dear
Parents, Sisters
And Friends

- Chetana S. Khetmal

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study



www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Acknowledgements

I am extremely happy to present this book on "Internet Technology" for my students of sixth semester Mumbai university Information technology branch. It is excellent feedback of my students which triggered me for writing this book.

I would like to take this opportunity to thank my mother and father for their immense support and encouragement. I am also thankful to my wife Kasturi Mali for valuable time of typing my thoughts on computer with the speed it comes in my mind. I am grateful to all my family members for their blessings.

There are number of other people who are indirectly responsible for successful completion of this book. Like many of my students and friends took time out of their busy schedules to provide peer reviews, suggestion and assistance. The reviewers include students (Tanvi, Mukund, Kaustubh, Komal, Pratik and all) of and faculties of various colleges. I would like to thank them for spending their valuable time in reviewing the book.

- Mahesh Mali

maheshmalisir@gmail.com

I would like to first thanks to Mr. Mahesh Mali who has triggered me to think one step ahead rather than just thinking about writing a book. He has helped me at each and every point and guided me a lot.

I would like to express my gratitude to my dearest father and mother for their encouragement. This mission was not able to be successful without help of my sisters and cousins. I am grateful to all my family members for their blessings. I express my gratitude to my friends who have boosted me from the start of this journey

I convey my sincere thanks to Management of K.C .College of Engineering and all the staff members of K.C .College of Engineering for their immense support due to which I have completed my very first operation of writing a book successfully.

I wish I would get suggestions and feedback from my all students for the betterment in this new task.

I am sincerely thankful to Sachin Shah and Sheetal Bhandari for helping and encouraging me in writing this book. It is very important to thank design team of TechMax Publication for their great assistance to make this book as good as it is.

Chetana Khetmal

khetmalchetana@gmail.com

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

About Authors

Mr. Mahesh Mali

He holds Bachelor of Engineering degree in field of Information technology engineering branch from Mumbai University with distinction. He is now pursuing Masters of engineering degree as a GATE Scholar. He has got International certification as "*Oracle Certified PL/SQL Developer Associate*".

He has performed the role of *Sr. Software Engineer* at Mastek Ltd. for more than 2 years. He was working as an *Assistant Professor* from last 5 years now, working with St. Francis Institute of technology (SFIT), Mumbai. He has around 8-9 years experience in teaching field. He has guided many technical projects of degree and diploma engineering.

He has written more then 18 books on technical topics like Relational databases, advanced databases and SQL and PLSQL for various course like Engineering, B.Sc.(IT),B.Sc.(CS) and Diploma of various universities.

Ms. Chetana Khetmal

Ms. Chetana Sudhakar Khetmal holds Bachelor of Engineering degree in field of Information technology engineering branch from Mumbai University with distinction. She is now pursuing Masters of engineering degree in computer engineering branch Mumbai University.

She is working as an *Assistant Professor* K.C.College of Engineering, Thane (E), Mumbai from last 2.5 years. She has around 4.5 years experience in teaching field.

She has presented technical papers on Networking, Data warehousing, MANET. Her special areas of interests are Networking, Software Engineering, Data warehouse, C, C++ etc. She likes to do some innovations in the teaching and learning process.

□□□

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Preface

The field of Internet technologies has evolved from a simple web application to an advanced client server systems. Knowledge about such systems has become an integral part of education in today's Information age. These concepts include all aspects of communication system design, socket programming and network system implementation. The developments in this technology over the last few years have produced more secure and powerful network which is more intuitive to use.

We have divided entire syllabus into small chapters which are easy to understand. We have attempted to present the entire material in a clear, concise and point wise manner which will be very simple for students.

We have made all possible efforts to make this book error free. However it is request to all students and faculties of various colleges in Mumbai University if you have any type of query on any of topic please feel free to mail me on below mentioned e-mail id, because that will help us to improve further. All types of feed back in future from students and faculties are welcome.

maheshmalisir@gmail.com

Chetana Khetmal

khetmalchetana@gmail.com

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Syllabus

UNIT I

Introduction: OSI Model, TCP/IP Protocol Suite, IPV 4 Addresses and Protocol and IPV6 Addresses and Protocol **(Refer chapter 1)**

UNIT II

Address Resolution Protocol (ARP), Internet Control Message Protocol Version 4 (ICMPv4), Mobile IP, Unicast Routing Protocols (RIP, OSPF and BGP)

(Refer chapters 2 and 3)

UNIT III

User Datagram Protocol (UDP), Transmission Control Protocol (TCP) **(Refer chapter 4)**

UNIT IV

Stream Control Transmission Protocol (SCTP), Host Configuration: DHCP, Domain Name System (DNS) **(Refer chapter 5)**

UNIT V

Remote Login: TELNET and SSH, File Transfer: FTP and TFTP ; World Wide Web and HTTP, **(Refer chapter 6)**

UNIT VI

Electronic Mail: SMTP, POP, IMAP and MIME, Multimedia

(Refer chapter 7)

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Chapter 1 : Introduction to Internet Technologies 1-1 to 1-46

Chapter 2 : Network Layer 2-1 to 2-22

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

CHAPTER 1

Introduction to Internet Technologies

Syllabus

- OSI Model
- TCP/IP Protocol Suite
- Network Layer
- IPv4 and IPV6 Addresses and Protocol

1.1 Introduction to Networks

- A computer network is a set of multiple computers or other hardware components interconnected by communication channels that allow sharing of resources and information between multiple users and processes.
- If in a network one process sends the data and other receives it then it is said to be they are in a network.
- The medium use for sending or receiving data is called as communication channel.

1. Client Computer :

- A client is a system that accesses the remote service on another computer using network.
- The computer that initiates communication is generally called as client computer.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

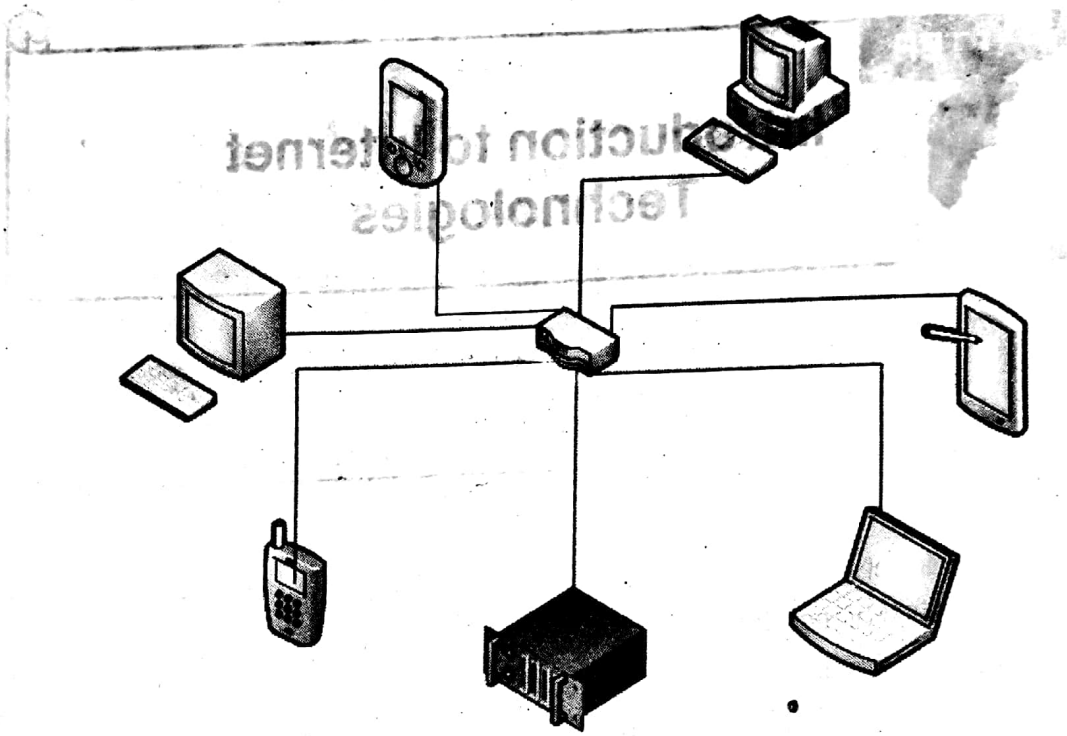


Fig. 1.1.1 Computer Network

2. Server Computer :

- Server is a computer program that provides services to other computer programs in the same or other computers on network.
- The computer that answers the client computer is generally called as server socket.

3. Client Server Architecture :

- Programs running on client machines make requests to a program (i.e. Server Program) running on a server such architecture is called as client server architecture.
- Client server architecture is work on basis of request response model.
- Client sends request to server and server replies to the request.

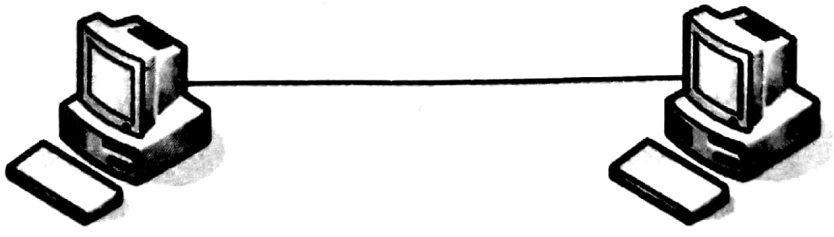


Fig. 1.1.2 : Client server architecture

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.2 Networking Standards

- The first idea of networking is put forwarded by ARPA (Advanced Research Projects Agency) in department of defence for communicating different computers with each other.
- In 1967, at the meeting of ACM (association of computing machines) ARPA has presented the innovative idea of ARPANET which is small network of computers.
- ARPANET uses the intermediate machine for transferring message from one machine to other called as IMP (Interface message processor).
- TCP/IP includes the concepts like encapsulation of data packets includes two protocols transmission control protocol and Internetworking protocol.

Standard Organisations

- ISO (International Standard Organisation)
- International Telecommunication Union Telecommunication Standards sector (ITU-T)
- American National Standard Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Electronic Industries Association (EIA)

International Forum

- Frame Relay Forum
- ATM Forum

Regulatory Agencies

- Federal Communications Commission (FCC)

1.3 OSI Model

a) Introduction :

- This model has dominated the sector of data communication and networking before 1990.
- Later on TCP/IP protocol suite became dominant and more popular in today's internet which was first successfully implemented networking model.
- The OSI model is established in 1947 which is multinational model which is agreed as international standard.
- This OSI model covers all aspects of network communication given by ISO standards.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- OSI model is network architecture which is interoperable and very flexible for multiple applications.
- It is a layered framework for designing complex network system which helps communication between multiple computers.

b) Layered Architecture :

- It consists of seven different layers through which data will pass for better communication.
- If one computer wants to send any message X to another computer then message should pass through all seven layers on both nodes, while intermediate node may have three layers of OSI layer.

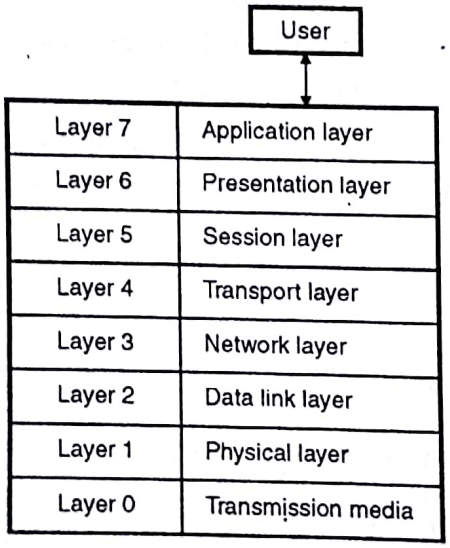


Fig. 1.3.1 : A seven layer ISO-OSI reference model

1.3.1 Exchange of Information using OSI Model :

a) Packaging information in Layers :

- Wrapping data packets

Each OSI layer of sender machine adds own information to packet it has received from previous OSI layer and pass entire packet to next OSI layer.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

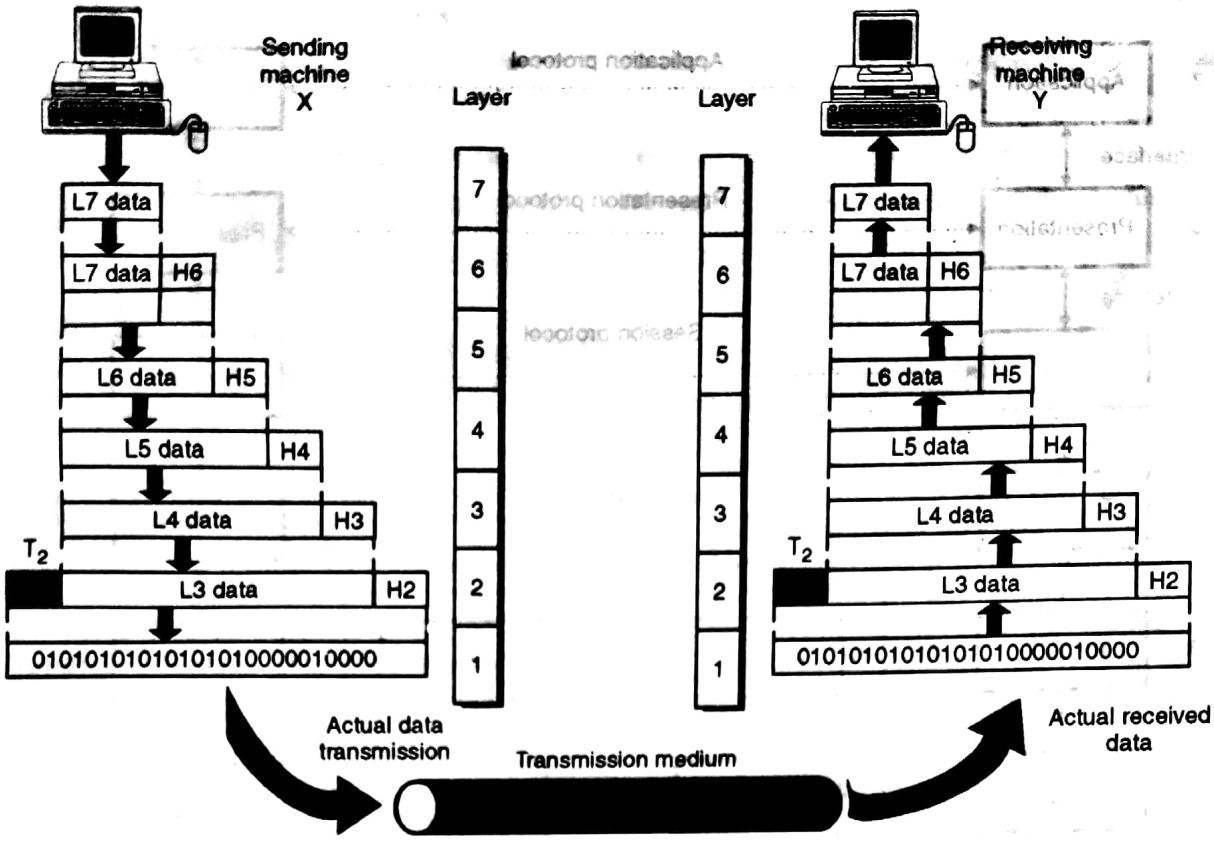


Fig. 1.3.2

- Unwrapping data packets

  OSI layer of receiving machine will remove the information added by corresponding layer on sender machine and pass remaining packet to above OSI layer. This process called as Decapsulation.

- **Example :** Layer 4 of receiver can only removes the information added by layer 4 of sender process and it applies for all other layers.

b) Modularity of OSI Model :

- The modularity is offered to network by providing well defined interfaces between two layers as shown in Fig. 1.3.3.
- The data packets are transferred from one layer to another layer above it or layer below it using these layer interfaces.
- Interface defines the information and services needed or provided by layer above it or layer below it.
- Implementation of interfaces will be required to change only if services required by above layer are changed.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

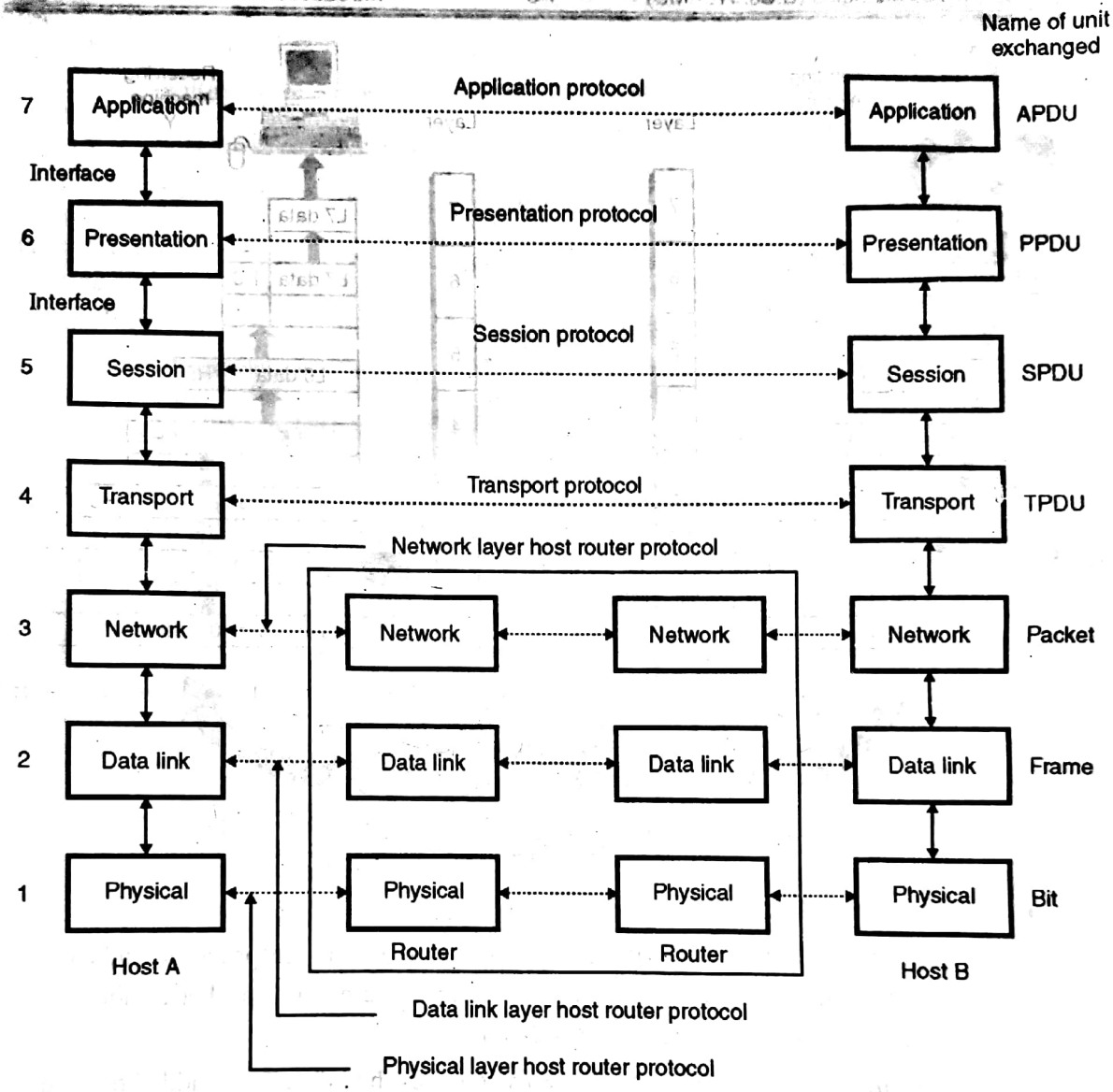


Fig. 1.3.3

c) Organising layers in groups :

- The seven layers of OSI are grouped into 3 subgroups as given below :
- Network Support Layer
  - It includes OSI layer 1 (Physical layer),Layer 2 (Data link layer) and Layer 3 (Network Layer)
  - These layers used in data migration from node to node like connection, addressing and timings including reliability of data)
  - It is mostly implemented using only software.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Users Support Layer
  - It includes OSI layer 5 (Session layer),Layer 6 (Presentation layer) and Layer 7 (Application Layer)
  - Allows interpretability between dissimilar software systems.
  - It is mostly implemented using combination of hardware and software.
  - Physical layer requires complete hardware.
- Transport Layer
  - It includes OSI layer 4 (Transport layer)
  - Takes care about information transferred from lower layer to upper layer are in same form.

d) Encapsulation :

- Any packet at level N is encapsulated in level N-1 and it applies for all other layers.
- E.g. Packet at level 4 is encapsulated in level 3 in this whole packet coming from level 3 is acts like a single integrated unit.

1.3.2 Layers of ISO - OSI Model :

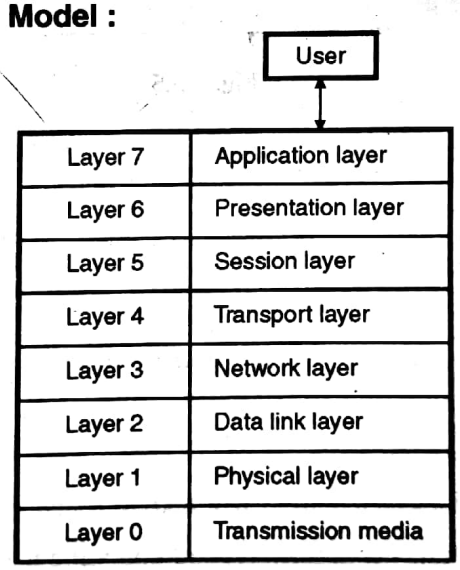


Fig. 1.3.4

1) Physical Layer :

a) Introduction :

- Physical layer concern with physical connection to network and transmission or reception of signals.
- It consists of transmission medium like connecting wires.
- Physical layer sending bits from one computer to another.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) Position :

- Physical layer is first layer in OSI model and it defines methods using which physical devices perform transmissions of signals.

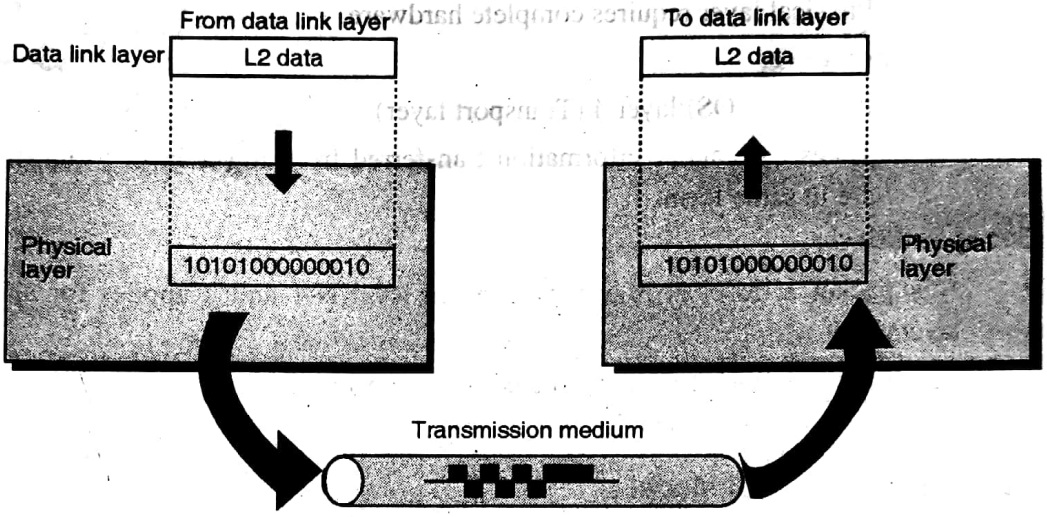


Fig. 1.3.5

c) Protocols :

- RS - 232
- RS - 449

d) Functions :

- It defines characteristics of interface or transmission media between various devices.
- **Transmission rate** - It defines number of bits transmitted per second and also defines how long it will take to transfer data.
- **Encryption** - It defines type of encoding used for transmitting signal.
- **Synchronization** - Sender and Receiver must be synchronizing at same bit level and data rate.
- **Physical Connection** - Layer deals with the network connection types like P to P configuration or multipoint configuration.
- **Mode of Transmission** - Data can be transferred using anyone of mode given below - simplex transmission, half duplex transmission or full duplex transmission.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Topology** - this later deals with how devices are connected to each other using physical topology like Bus topology, Ring topology, Mesh topology or Star topology.
- **Bandwidth** - It deals with a physical transmission media bandwidth.

e) Devices Used :

- Hubs
- Connecting wires and connector
- Transmitter and Receivers
- Repeater etc.

2) Data Link Layer :

a) Introduction :

- It responsible for node to node delivery of data packets.

b) Position :

- It accepts data packets from networks layer and forms frames which will be given to physical layer for transmission.

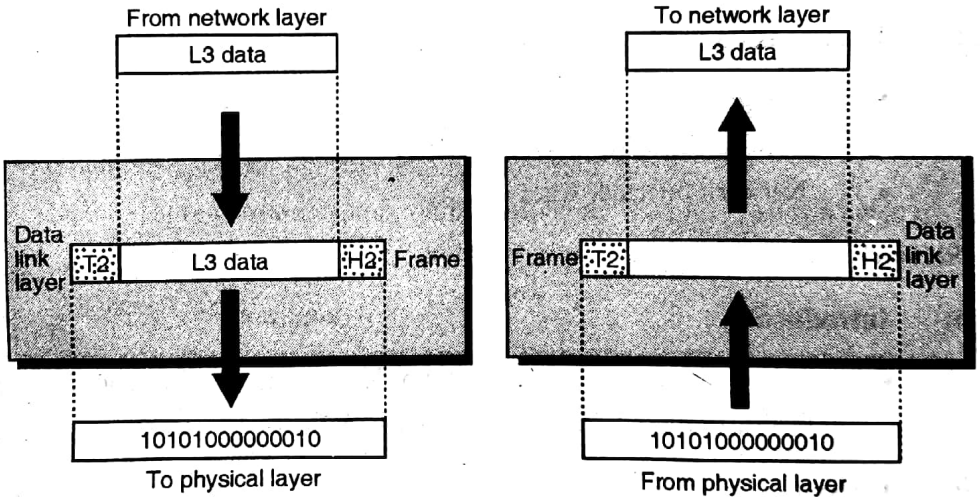


Fig. 1.3.6

c) Protocols :

- HDLC
- SDLC
- X.25

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

d) Functions :

- **Data frame** - This layer divides data packets in to manageable pieces of data which is also called as Data frame.
- **Addressing** - The layer will define header for each frame which contents physical address of Sender and Receiver.
- **Flow control** - It manages data rate to avoid fast data transmission from over running a slow receiver by data buffering.
- **Error control** - Layer achieves error control by adding trailer at the end of the frame. It also identifies Lost, Duplicate or Damage frame and handles it by retransmission of frame or just by avoiding them.
- **Access Control** - Data link layer determines which device out of many will take control over a link at given point of time. For access control data link layer divided in two sub layers,
- **Logical Link Control (LLC)** - It establishes and maintains link between various communicating devices.
- **Media Access Control (MAC)** - It controls sharing of media channel between multiple devices. MAC address use to form logical link between multiple computers on same LAN.

e) Devices Used :

- Bridges
- Intelligent Hubs
- Network Interface Card (NIC)

3) Network Layer :

a) Introduction :

- Network layer mainly deals with delivery of packets from source node to destination node using various network links.

b) Position :

- It accepts data from transport layer adds own header which contains addressing information and this data is now called as Data Packet will be transferred to data link layer.
- On receiving data frame from data link layer removes header appended by source if receiving computer is actual receiver of data.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

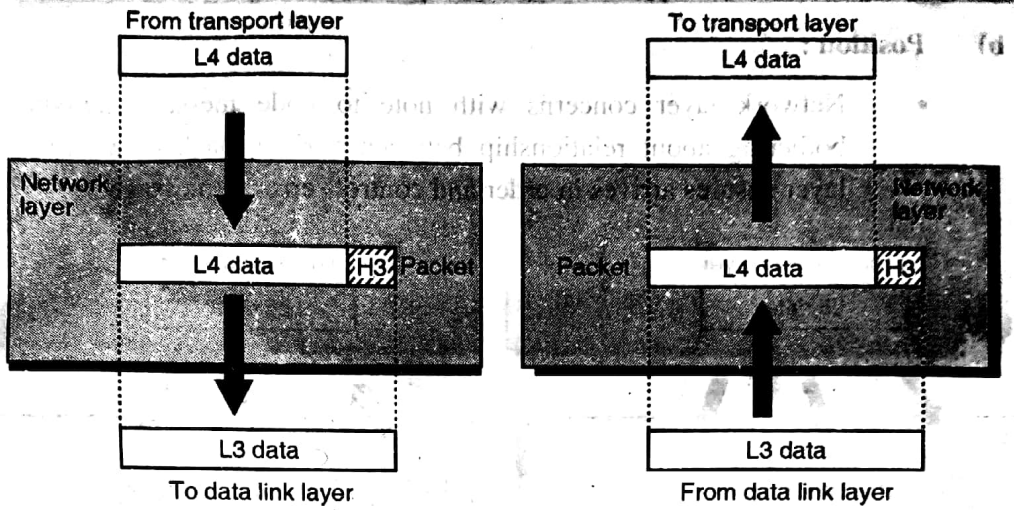


Fig. 1.3.7

c) **Protocols :**

- ICMP
- IGMP
- ARP
- RARP

d) **functions :**

- **Addressing** - Network layer translate logical address (IP address) in to physical machine address.
- **Switching** - It concerns the type of switching used like circuit switching or packet switching
- **Message priority** - It offers quality of service by deciding priority of messages.
- **Data fragmentation** - It divides larger data packets into smaller packets if required.

e) **Devices Used :**

- Routers
- Gateways

4) Transport Layer :

Q. Describe the function of the transport layer in the OSI model MU - April 2013

a) **Introduction :**

- This layer ensures delivery of complete message from source node to destination node i.e. process to process delivery of message with error detection and recovery.
- Process means any application programme running on host node.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) Position :

- Network layer concerns with note to node message delivery without bothering about relationship between various packets whereas transport layer ensures arrives in order and controls error in message.

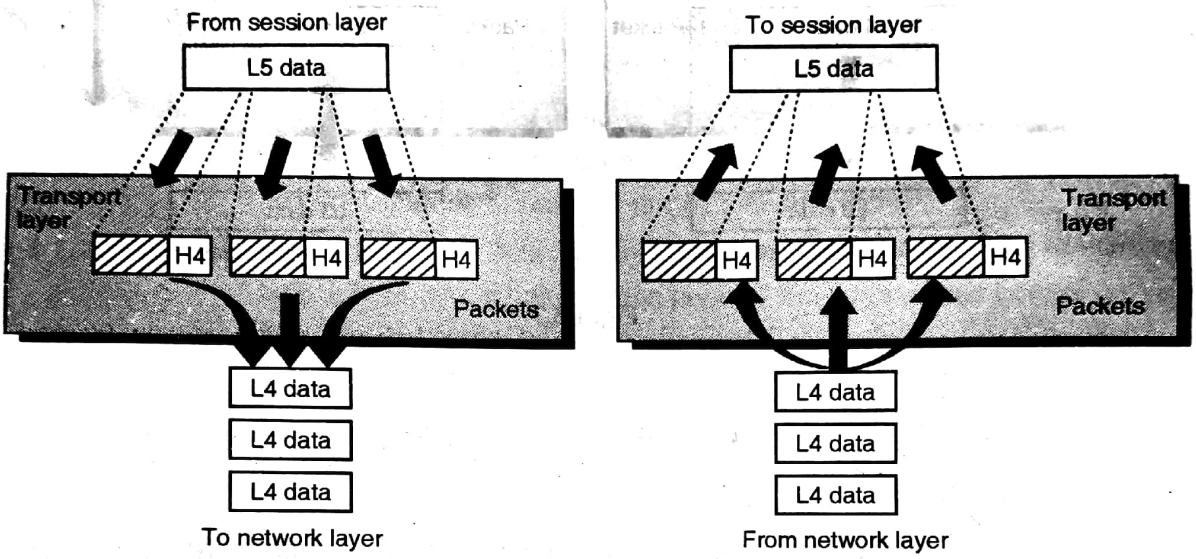


Fig. 1.3.8

c) Functions :

- **Segmentation** - It divides message into manageable date segment which contents unique segment number to each segment which way will help us in reassembling message at receiver.
- **Connection** - Transport layer can be connectionless or connection oriented.
- **Flow Control** - Layer Performs end to end flow control.
- **Error Control** - It makes sure that message arrives without any error.

5) Session Layer :

a) Introduction :

- This layer creates, maintains and synchronizes the communication between various communicating systems.

b) Position :

- It accepts from transport layer and adds synchronization points to stream of data or it may removes synchronization point at the receiver site.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

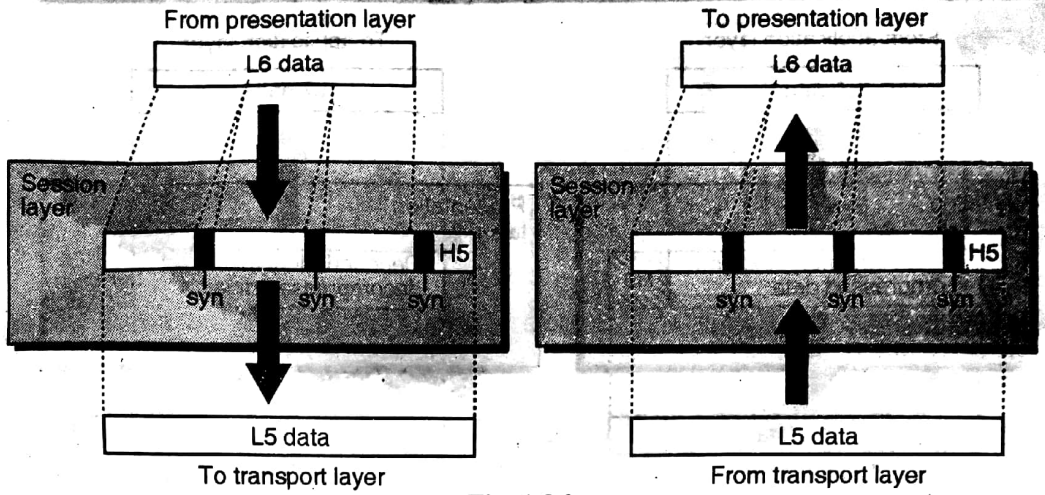


Fig. 1.3.9

c) Protocols used by all higher layers after this layer :

- FTP
- HTTP
- DNS
- SLTP
- SMTP
- SNNP
- TELNET etc

d) Functions :

- **Synchronization** - It allows process to add check point i.e. synchronization point into data stream. It will be used in case of failure the data will be retransmitted from particular check point.
- **Dialog Control** - Dialog means exchange of messages between various interested systems. Dialog control will controls communication between two processes in communication system which transfers data in full duplex and half duplex mode.

6) Presentation Layer :

a) Introduction :

- Presentation layer takes care of syntax of information to be exchange between various systems.

b) Position :

- The presentation layer will append its own header to data it accepts from higher levels.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

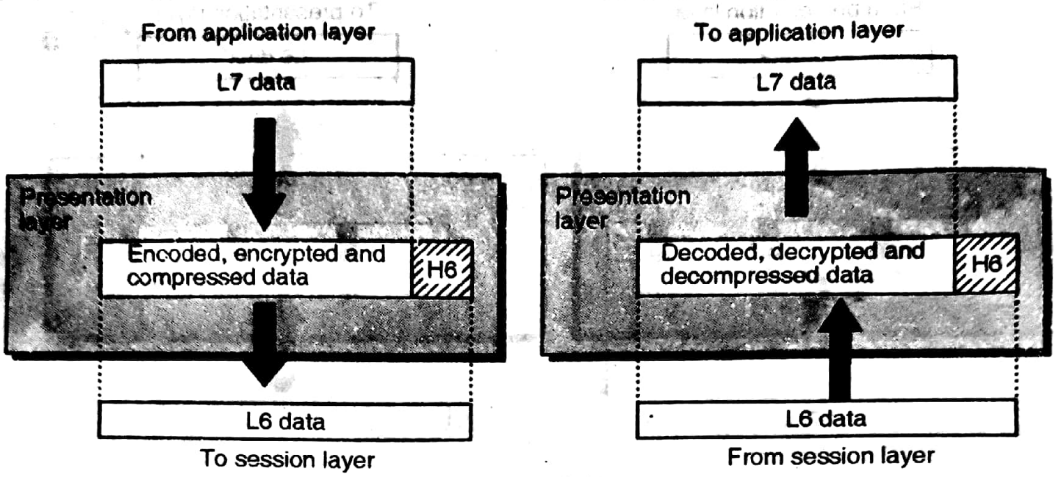


Fig. 1.3.10

c) Functions :

- **Translate data** - It translates data which require by receiving computer without protocol conversion.
- **Data Compression** - It reduces memory space require by the information for faster data transmission.
- **Data encryption** - It encrypts data for security and privacy of information over the transmission channel.

7) Application Layer :

a) Introduction :

- This layer helps user to access networking resources like database, email, files directly with help of user application.
- It allows one application to communicate another application on other computer as like they are situated on same computer.

b) Services :

- X.400 – message handling service
- X.500 – directory service
- FTAM – file handling and management service.

c) Position :

- It appends own header for accessing services mentioned above.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

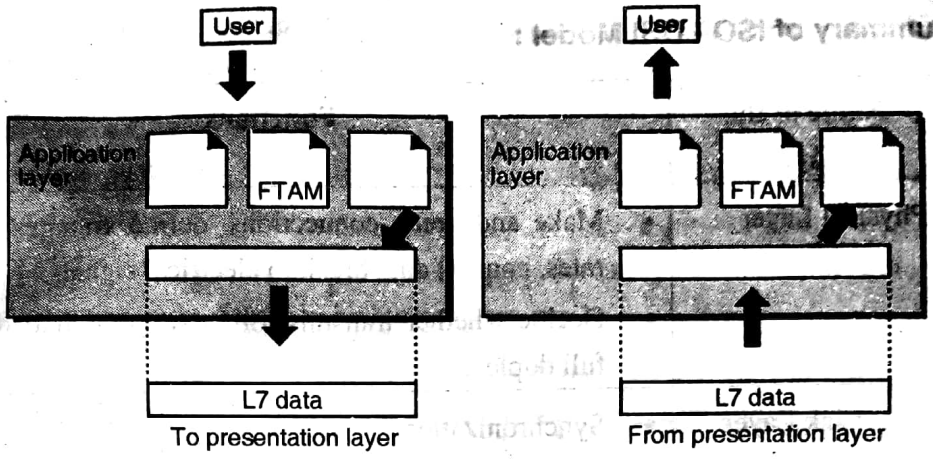


Fig. 1.3.11

d) Functions :

- **FTAM** - It allows user to access various files transfers and manages them in remote computing environment.
- **Mail Service** - The layer provide basis for email forwarding storing and retrieving it.
- **Directory Services** - This layer will provide access to worldwide information about various objects and services.
- **Virtual Terminal** - It allows remote login to other computers and work like own computer over the network.

1.3.3 Merits of OSI Model :

- It is layered architecture clearly distinguishes between the services, interfaces and protocols.
- The protocols in OSI model can be easily replaced by new protocols as the technology changes.
- OSI model is truly a general model which can be easily applicable to various protocol stacks.
- OSI model supports both connection oriented as well as connectionless services.

1.3.4 Demerits of OSI Model :

- OSI model does not uses sessions and presentation layers much.
- OSI model was developed before the protocols were invented. So there is a problem of fitting protocol into OSI model.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.3.5 Summary of ISO - OSI Model :

Level	Name of the Layer	Functions
1.	Physical Layer	• Make and break connections, define voltages and data rates, convert data bits into electrical signal. • Decide whether transmission is simplex, half duplex or full duplex.
2.	Data Link Layer	• Synchronization, • Error detection and correction. • To assemble outgoing messages into frames.
3.	Network Layer	• Routing of the signals • Divide the outgoing message into packets • Act as network controller for routing data.
4.	Transport Layer	• Decides whether transmission should be parallel or single path • Multiplexing, segmenting the data, • Break data into smaller units for efficient handling
5.	Session Layer	• To manage and synchronize conversation between two systems. • It controls logging on and off, user identification, billing and session management.
6.	Presentation Layer	• It works as a translating layer. • Encryption and decryption • Data compression
7.	Application Layer	• Retransferring files of information • LOGIN, password checking etc.

1.4 TCP/IP Protocol Suite Model

a) Introduction :

- This reference model was used earlier by ARPANET and then it is being used in the Internet.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- TCP/IP model included by many universities and government installations using the leased telephone lines. Later on the satellites and radio networks were added to it.
- These protocols suite describe the transfer of data between multiple host computers on Internet.
- TCP/IP suite offers a simple naming and addressing scheme using which different resources on Internet can be located very easily.
- TCP protocol is very much helpful for transferring large packets also over the network by just dividing it into a sequence of packets and each is put into an IP packet.
- In TCP the packets reach to destination but it is not necessary that they should follow the same path. At the destination the TCP software reconstructs the packets into a complete message.

1.4.1 Layers of TCP/IP Protocol Suite Model :

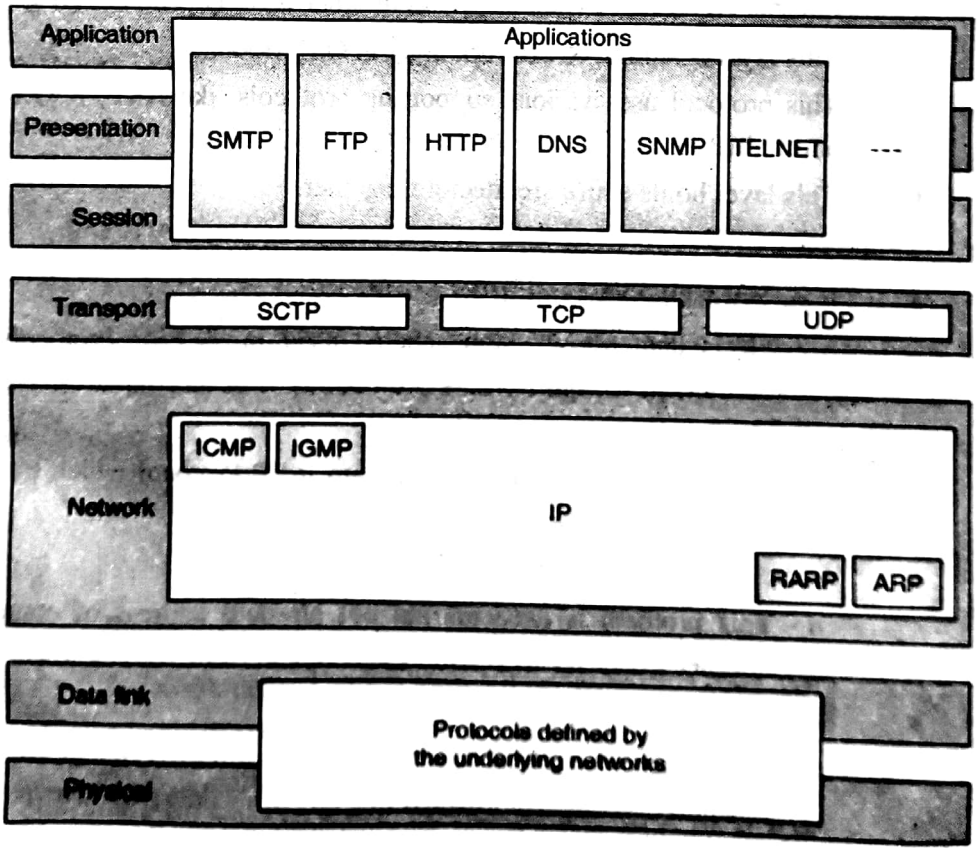


Fig. 1.4.1 : TCP IP protocol stack

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1) Host to Network Layer :

a) Introduction :

- This is lowest layer in TCP - IP Model.
- This layer is changes from host to host and layer to layer

b) Protocols :

- Advance Research Projects Agency Network (ARPANET)
- Pocket Radio
- SATNET LAN

c) Functions :

- This layer changes as implementation and vender changes.
- Functions are not defined clearly in protocol suite.

2) Network Layer / Internet Layer :

a) Introduction :

- Internet Layer in TCP / IP supports internetworking protocol (IP).
- This layer is similar to network layer in OSI Model.
- This protocol uses various supporting protocols like ARP, RARP, ICMP, and IGMP.
- This layer holds entire architecture together.

b) Protocols :

- Internetworking Protocol (IP)
  - It is data transmission scheme used in TCP/IP Protocols this is unreliable connectionless protocol as it do not have error checking technique.
  - Data Packet is called as datagram in IP Protocol which transported independently on network.
- Address Resolution Protocol (ARP)
  - This protocol is used to find out physical address of computer on internet whenever its IP Address (Logical Address) is known.
- Reverse Address Resolution Protocol (RARP)
  - This protocol is used to find out IP Address (Logical Address) of computer on internet whenever its physical address is known.
- Internet Control Message Protocol (ICMP)
  - This protocol is used by computers and getaways to notify datagram errors and queries back to sender.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Internet Group Message Protocol (IGMP)
  - This protocol is used to transfer same message to all recipients computers in a group.

c) Functions :

- ***Packet Transfer*** - The layer sends packets to any network and it will travel indecently towards destination.
- ***Packet Ordering*** - The order in which Packets are sent may be different at receiver end. The higher layer will arrange them in proper order.
- ***Internet Protocol*** - The network layer defines packet format and protocol which is called as Internet Protocol (IP).
- ***IP Packet Delivery*** - The layer is responsible for delivery of IP Packets Routing of packets and congestion control.

Application layer	TELNET, FTP, SMTP, DNS, HTTP, NNTP
Transport	TCP, UDP
Internet (Network)	IP
Host-to-network	ARPANET, SATNET LAN, packet radio

3) Transport Layer :

Q. Explain Stop-and-wait Protocol and G0-Back-N Protocol in the transport layer. MU - April 2013

a) Introduction :

- This layer is responsible for process to process message delivery.
- The layer performs functions with help of two protocols TCP and UDP.
- SCTP is newly device transport layer protocol for sum new applications.

b) Protocols :

- User datagram protocol (UDP)
  - It is process to process protocol which only inserts Port address, length information and error control to data coming from higher layers.
- Transmission Control Protocol (TCP)
  - This Protocol is reliable connection oriented protocol which establishes connection before sending or receiving data.
  - The data units are divided into segment by TCP Protocol including sequence number of each segment which is used for reordering data.
- Stream Control Transmission Protocol (SCTP)
  - This protocol combines best features of TCP and UDP Protocols.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- It is used for new applications.
- Stop n wait protocol:

- It is connection-oriented protocol. Stop n wait protocol uses both flow and error control.
- In this protocol the sender and the receiver both uses a sliding window of size 1 and only one packet and one acknowledgment can be in the channels at any time.
- It is called as Stop n wait because; the sender sends one packet at a time and waits for an acknowledgment before sending the next packet.
- Checksum is added to each data packet for checking the corruption in packet. When a packet arrives at the receiver site, checksum is checked. If its checksum is incorrect, it means the packet is corrupted and silently discarded. The receiver sends a signal to the sender which specifies that a packet was either corrupted or lost.
- Before sending packet sender sets one timer if an acknowledgement arrives before expiration of timer than timer is stopped and sender ready to send next packet through the channel.
- If the set timer expires and still acknowledgement does not arrives than sender resends the packet by assuming the packet may be lost or was corrupted.
- Hence sender needs to keep copy of a particular packet until its acknowledgement arrives.

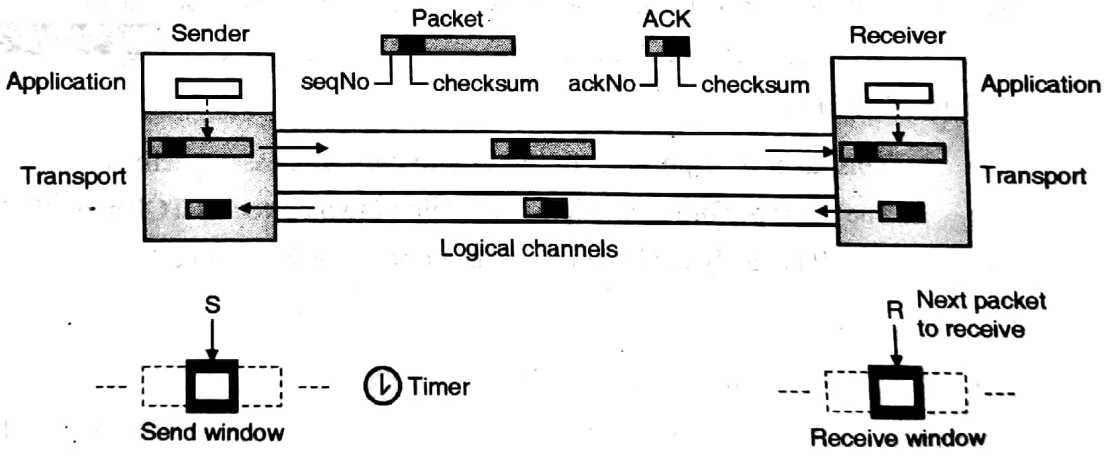


Fig. 1.4.2

- Go back N Protocol :
- To improve the efficiency of transmission by forwarding multiple packets while the sender is waiting for acknowledgment we are able to keep communication channel busy.
- The Go-Back-*N* (GBN) protocol fulfils this requirement. The Go-back-*N* *helps to* send several packets before receiving acknowledgments of current

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

packet. Due to this approach several data packets and acknowledgments can be in the channel at the same time.

- One limitation in Go-Back-*N* is that the receiver only buffers one packet at any time
- Hence in this protocol also sender keeps a copy of the sent packets until the acknowledgments arrive.

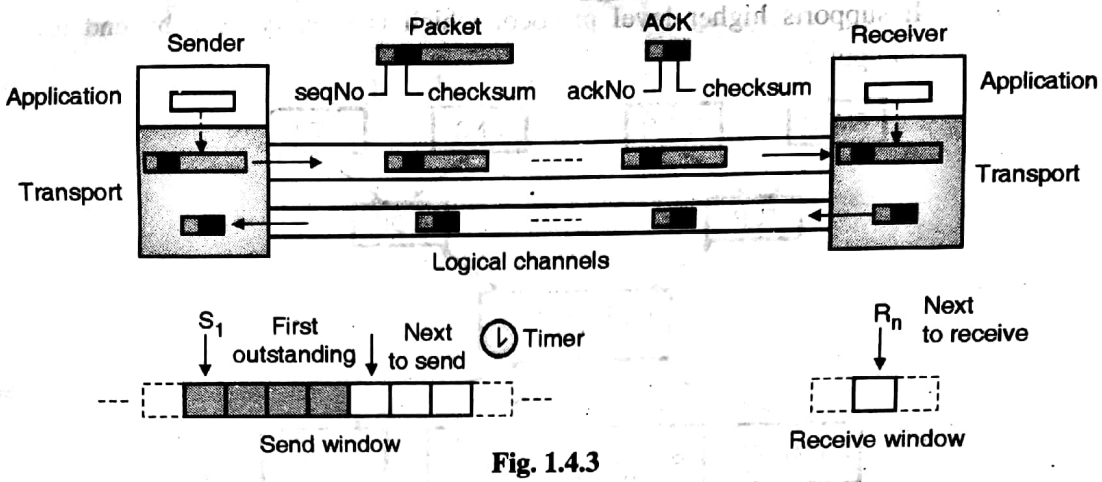


Fig. 1.4.3

c) Functions :

- ***Process to process message delivery*** - This layer is responsible for process to process message delivery unlike IP Protocol which delivers message from one computer to another computer. This layer delivers message to respective process of destination computer.
- ***Packet sequencing*** - The data units are divided into segment by TCP Protocol including sequence number of each segment which is used for reordering or sequencing data.

4) Application Layer :

a) Introduction :

- The layer performs the entire task performed by Session Layer, Application Layer and Application Layer is OSI model.

b) Protocols :

- Domain Name Service (DNS)
  - It is used for converting Internet Address into IP Address of respective Web Server.
- File Transfer Protocol (FTP)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- This Protocol is used for sharing data between multiple computers on internet.

- Simple Mail Transfer Protocol (SMTP)
  - It is used for sending electronic mail (email) to the intended recipient
  - POP 3 i.e. Post Office Protocol is used for receiving email.

c) Functions :

- It supports higher level protocol which is directly used by end user of computer.

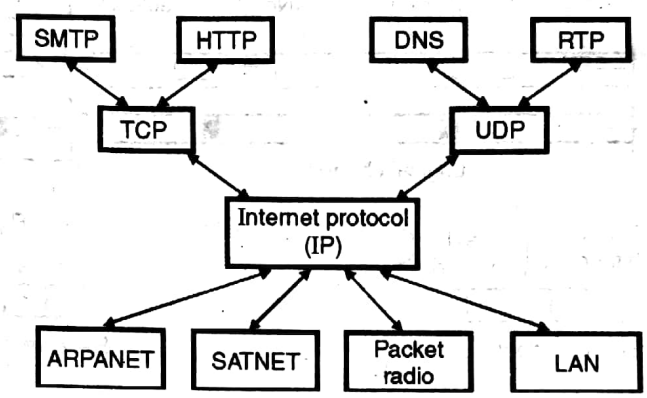


Fig. 1.4.4 : Protocols and networks in the TCP/IP model

1.4.2 Demerits of TCP/IP Protocol Suite Model :

- TCP/IP protocol suite does not distinguish clearly the concepts of service, interface and protocol.
- This model is not at all general model so, can not describe any other protocol stack.
- The host-to-network layer is not a layer but it is a simple interface.
- The TCP/IP model does not mention about physical and data link layers. A proper model should include both as separate layers.

1.5 Comparison of OSI and TCP/IP Models

1) Similarities between OSI and TCP/IP models :

a) ***Functionality*** - Both the models the layers have approximately the same functionality.

b) ***Layered Architecture*** - Both models uses the layered architecture.

c) ***Services*** - The transport layers and the layers below it provide transport services independent of networks and layers above it are application oriented.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2) Relationship between OSI and TCP/IP models :

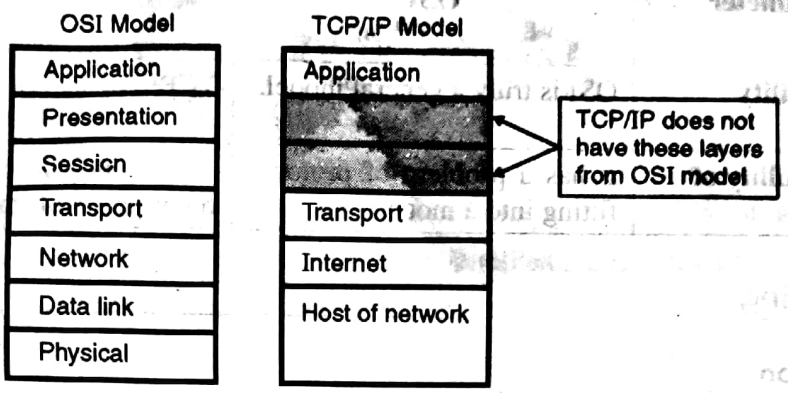


Fig. 1.5.1 : Relationship between OSI and TCP/IP models

3) Distinguishing between OSI and TCP/IP models :

Table 1.5.1 : Difference between OSI and TCP/IP model

Sr. No.	Parameter	OSI	TCP/IP
1.	**No. of Layers**	Contains 7 layers	Contains 4 layers
2.	**Transport Layer**	It guarantees delivery of packets.	It does not guarantee delivery of packets.
3.	**Approach**	Horizontal approach.	Vertical approach.
4.	**Session layer**	Separate session layer.	No session layer, functions carried out by transport layer.
5.	**Presentation layer**	Separate presentation layer.	No presentation layer, functions carried out by application layer.
6.	**Mode of service provided by network layer**	Network layer provides both connectionless and connection oriented services.	Network layer provides only connection less services.
7.	**Services, interfaces and protocols**	It defines the services, interfaces and protocols very clearly with a clear distinction between them.	It does not clearly distinguish between service, interfaces and protocols.
8.	**Protocol changes**	The protocols are better hidden and can be easily replaced as the technology changes.	It is not easy to replace the protocols.

www.MumbaiBScITStudy.Com

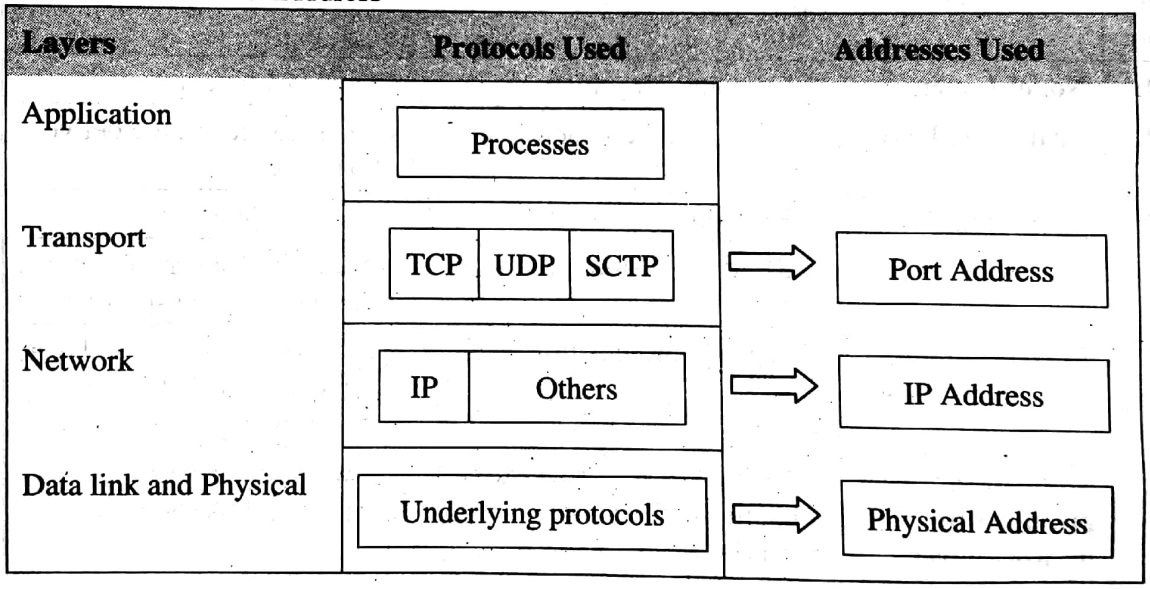
Mumbai B.Sc.IT Study

Sr. No.	Parameter	OSI	TCP/IP
9.	**Applicability**	OSI is truly a general model.	TCP/IP can not be used for any other application.
10.	**Compatibility of model**	It has a problem of protocol fitting into a model.	The model does not fit any other protocol stack.

1.6 Addressing

1) Introduction :

- Internet uses three different levels of addressing to use along with TCP/IP Protocol suite.
- The various addresses uses are as below :
  - Physical Address / Hardware Address
  - Logical Address / IP Address
  - Port Address



2) Physical Address :

- Physical address is also called as MAC address or Hardware address or Link Address.
- Physical address is 48 bits long and it is set by manufacturer.
- It will be unique for any network or LAN.
- The host and routers are uniquely identified by using physical address at physical layer.
- It is local address and it is implemented in hardware.
- Ex. B4:6B:A4:69:73:BA

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3) Logical Address :

- Logical address is called as IP address in TCP/ IP protocol suit.
- It is used for universal communication which is almost independent of underlying physical networks.
- Different network can have different formats for physical address but, using logical addressing host can be identified uniquely regardless of network used.
- Logical address is 32 bits long and it is implemented using software.
- Logical address is set by the operating system of machine.
- The hosts and routers are differentiated at Network layer by using logical address of machine.
- Types
  - Unicast : One recipient only
  - Multicast : Group of recipients
  - Broadcast : All recipients in network
- Ex. An internet address in IPv4 is 32 bit long as below,

192 . 168 . 0 . 32

4) Port Address :

- A port is a 16-bit number.
- It is used by the host-to-host protocol to identify which higher level process (Like TELNET, FTP etc.) on receiving host must accept incoming messages coming from process of sending host.
- If message is transferred from computer A using FTP (File transfer protocol) then it should be received by FTP (File Transfer Protocol) on receiving computer. It is possible that many such protocols or processes may be running on same machines.
- Whenever any process wants to communicate with another process, it identifies itself to the TCP/IP protocol suite by one or more ports.
- Port numbers are divided into three different categories as given below:
  - Ports 0 through 1023
    1. They are called as well known ports.
    2. They are associated with services in a static manner.
    3. E.g. HTTP servers would accept requests at port 80.
    4. The "well-known" ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) and most systems can only be used by system programs run by privileged users.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Port numbers 1024 - 49151
  1. They are called as registered port numbers.
  2. They generally used for multiple purposes.
  3. These port numbers are not controlled by the IANA and systems can be used by ordinary user-developed programs.
- Port 49152 - 65535
  1. They are Dynamic and private port numbers
  2. No services associated with them.

1.7 IPv4

a) Introduction :

1. IPv4 is the fourth revised form of the Internet Protocol (IP) and the first version of the protocol to be widely used for deployment.
2. IPv4 is a connectionless protocol generally used on packet-switched Link Layer networks like Ethernet.
3. IPv4 does not guarantee delivery or does not ensure proper sequencing to avoid of duplicate delivery.
4. IPv4 is 32-bit addressing scheme given as below,

192 . 168 . 0 . 32

b) IPv4 Header Format :

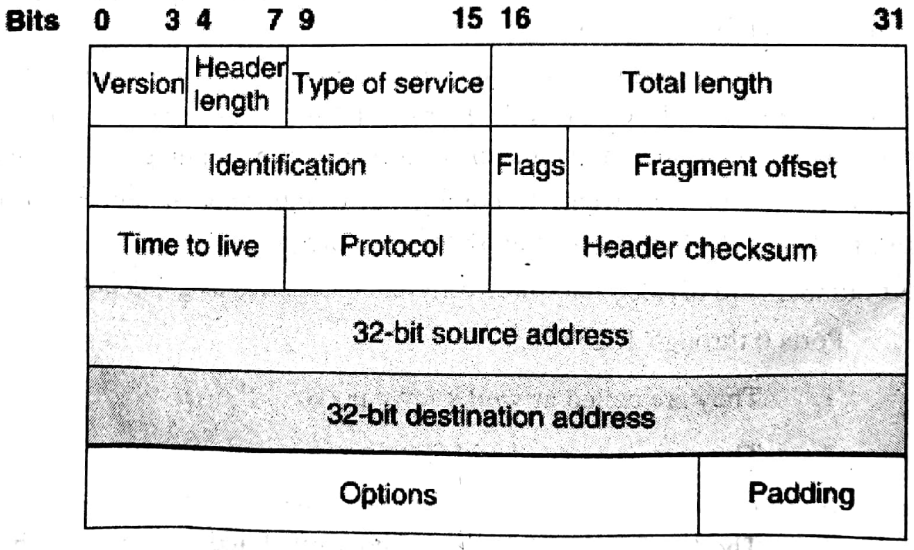


Fig. 1.7.1

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1. Version :

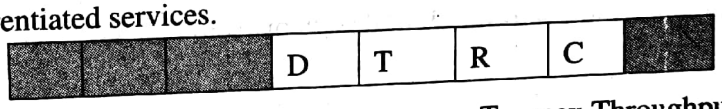
- It is a 4 bit field defines version of IP (4 or 6)
- For IPv4 ,field value is 0100
- All packets other then this value will be discarded.

2. HLEN :

- Header length field contains length of header file of datagram
- As datagram length is variable between 20 to 60 Bytes.
- Without options field header length will be 20 Bytes.
- Hence, field contains value $(5 \times 4 = 20) = 0101$
- This value is always multiple of 4
- Maximum HLEN will be 60 as field contains 15 $(15 \times 4) = 1111$

3. Service Type :

- In original IP datagram the field was service type now this field is referred as Differentiated services.



D = Minimize Delay

T = max Throughput

R = Max Reliability

C = Minimize (OS)

E.g. -

ICMP	0000	-	Normal
SNMP	0010	-	Max Reliability
Telnet	1000	-	Min delay
FTP	0100	-	Max Throught

4. Total length :

- This field of 16 bit defines total length in bytes.
- Length of data = Total length – HLEN
- Max total length is = $2^{16} - 1 = 65535$ bytes, so it can contains 20 to 60 bytes of data.

5. Identification :

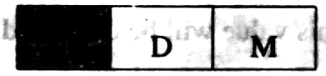
- This field of 16 bits identifies source of packet.
- The combination of identification field sequence number and source IP address must uniquely define a datagram when it leaves source to guarantee the uniqueness of IP protocol.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

6. Flags :

- This is 3 bit field out of which 1 is reserved for future use.



D - Do not fragment

M - More fragments

7. Fragmentation Offset :

- This field shows relative position of fragment with respect to entire datagram.
- It is offset of data in original datagram measure in units of 8 bytes.

8. Protocol :

- This field defines higher level protocols with help of IP layer defines final destination of protocol to which IP datagram should be delivered.
- E.g.

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Q. Find the error, if any, in the following IPv4 addresses **MU - April 2013**

i. 127.045.112.27

Ans. : There are no leading zeroes in dotted-decimal notation of Ip address (045).

ii. 12.24.35.7.8

Ans. : The IP address is of 32 bits only with four octet or four bytes address. In given address there are five octets which is not possible.

iii. 10110011.23.45.234

Ans.: IP address can be made up of either by Binary notation or by using decimal notation it can not be the combination of both in one address.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

iv. 76.27.256.23

Ans. : In dotted-decimal notation, each number is less than or equal to 255; 256 is outside this range.

v. A23.56.78.5

Ans. : Alphabet is not allowed in IP address

1.7.1 IP Addresses :

Introduction :

- Logical address is called as IP address in TCP/ IP protocol suit.
- It is used for universal communication which is almost independent of underlying physical networks since an IP addresses are unique.
- Different network can have different formats for physical address but, using logical addressing host can be identified uniquely regardless of network used.
- IP addresses are 32 bits long and it is implemented using software.
- IP addresses are set by the operating system of machine.
- The hosts and routers are differentiated at Network layer by using IP addresses of machine.

Address space :

Addresses specified by an IP protocol define address space. An address space specifies the total number of addresses used by protocol.

The rule used for address space considerationis "If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 and 1) and N bits can have 2^N values".

The address space of IPv4 is 2^{32} because it is a 32 bit address.

Notations :

There are three methods for showing an IP addresses:

Binary :

- In the binary method, IP address is specified as 32 bits.
- IP address is referred as 4- octet address or 4- byte address.
- To make it more readable and to be in standard format one or more zeros are inserted between each octet i.e in 8 bits.
- For example the IP address with binary notation is shown below :

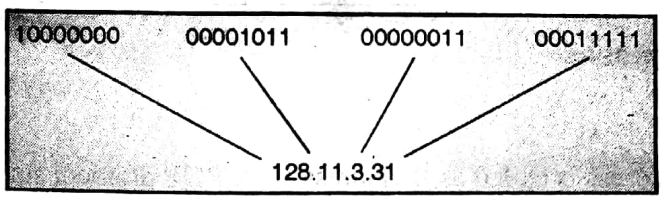
  01110101 10010101 00011101 11101010

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Dotted- Decimal :

- To make IP address more compressed and easy to read, IP addresses are written by separating the bytes using decimal points.
- Each number in the octet is in between 0 and 255.
- As per shown in the example the dotted notation is easier;



Hexadecimal :

- The IP addresses shown in binary also referred using hexadecimal notation for better understanding;
- Each hexadecimal digit is equivalent to four bits of IP address.
- Since IP address is of 32 bit it has 8 hexadecimal digits.
- It is useful in network programming.

0111 0101 1001 0101 0001 1101 1110 1010

75 95 1D EA

0x75951DEA

Example: Change the following IP address from binary notation to dotted-decimal notation.

10000001 00001011 00001011 11101111

129.11.11.239

Example: Change the following IP address from dotted-decimal notation to binary notation.

111.56.45.78

01101111 00111000 00101101 01001110

Example : Find the error, if any, in the given IP address: -111.56.054.87

There should not be leading zeroes in dotted-decimal notation (054).

Example: Find the error, if any, in the given IP address: - 127.65.310.0

In dotted-decimal notation, each number is less than or equal to 255; 310 is outside this range.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.7.2 Classful Addressing :

- Ipv4 is classified in to various classes by considering netid and hosts that can be connected to the particular address
  - Netid and Hostid:
  - Network address:
- It is the beginning address of each block.
- It can be found by applying the default mask to any of the addresses in the block (including itself).

  It specifies the netid of the block and sets the hostid to zero.

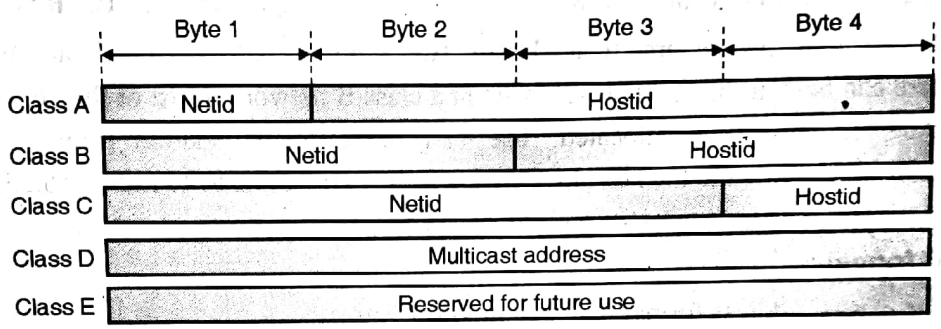


Fig. 1.7.2 : Class with Netid and Hostid

- The IP addresses are classified into 5 types as follows :

  1. Class A 2. Class B 3. Class C 4. Class D 5.Class E

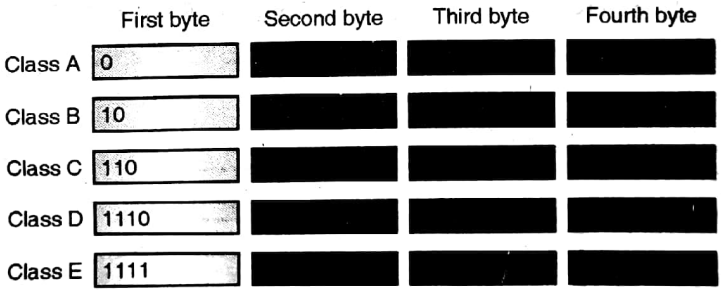


Fig. 1.7.3 : Class in binary Notations

- The formats used for IP address are as shown in Fig. 1.7.3.

Class A Format :

- The IP address for class A networks is shown in Fig. 1.7.4(a).
- The network field is 7 bit long as shown in Fig. 1.7.4(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 126.
- But the host numbers will range from 0.0.0.0 to 127.255.255.255.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The "0" in the first field identifies that it is a class A network address.

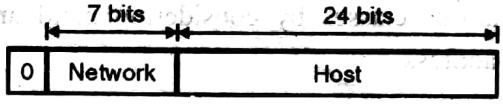


Fig. 1.7.4.(a) : Class A IP address formats

Class B format :

- The class B address format is shown in Fig. 1.7.4 (b)
- The first two fields identify the network id, and the number is in the 128 - 191.

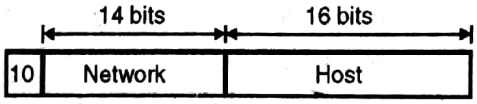


Fig. 1.7.4 (b) : Class B format

- Class B networks are large than Class A. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65,534 (216-2) hosts in a class B network. Most of the 16,382 class B addresses have been allocated. The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.
- **Example :** 128.89.0.26, for host 0.26 on net 128.89.

Class C format :

- The class C address format is shown in Fig. 1.7.4(c).

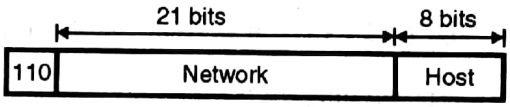


Fig. 1.7.4 (c) : Class C format

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 1.7.4 (d).

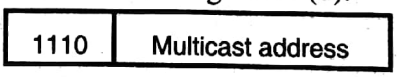


Fig. 1.7.4 (d) : Class D format

- The class format allow for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 1.7.4 (e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

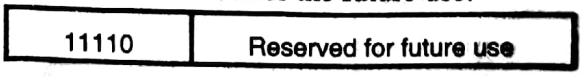


Fig. 1.7.4 (e) : IP address for class E network

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IP address is 255.255.255.255.

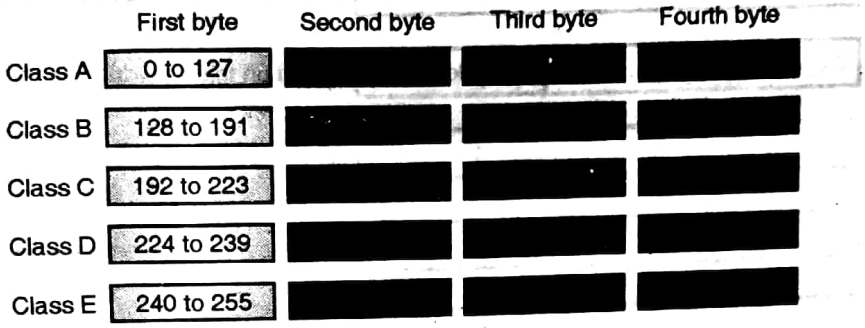
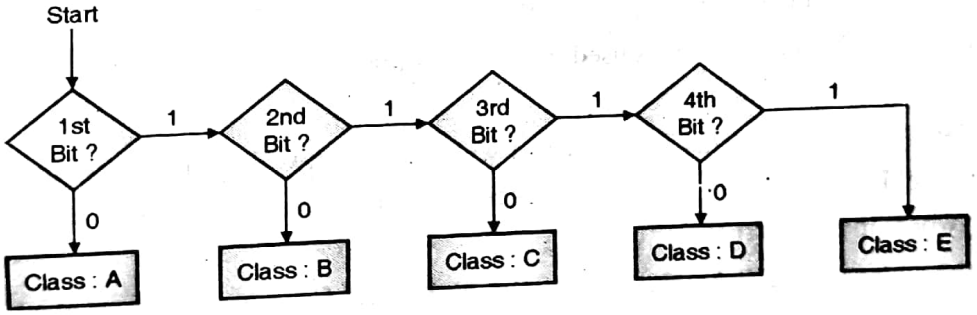


Fig. 1.7.5 : Class in decimal Notations

Finding the address class :

- To find out the network address by using the given flow graph is very fast and useful.
- We should consider the give bits of address and check from start condition;
- If 1st bit is 0 than it belongs to class A if it is not 0 means
- If it is 1 than check the 2nd bit if it is 0 than address is of class B if 2nd bit is 1 than check 3rd bit and the process goes on as per the flow mentioned in the given figure.



Q. Find the netid of the following IP addresses MU - April 2013

i) 114.34.2.8 Net id: 114 from class A

ii) 132.56.8.6 Net id: 132.56 from class B

iii) 208.34.54.12 Net id: 208.34.54 from Class C

iv) 251.34.98.5 Class E ; No Net id

v) 129.14.6.8 Net id: 129.14 from class B

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.7.3 Special IP Addresses :

- Fig. 1.7.6shows some special IP addresses.

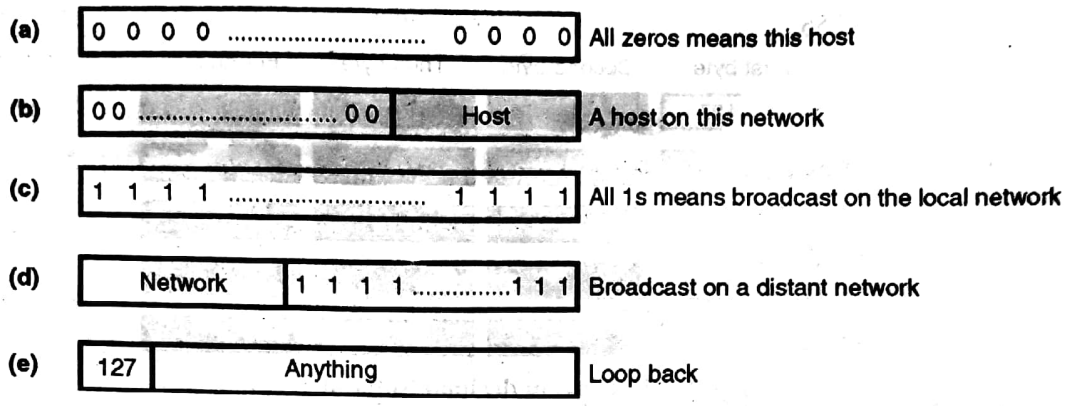


Fig. 1.7.6 : Special IP addresses

- All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- The IP addresses with 0 as the network number refer to their own network without knowing its number as per Fig. 1.7.6(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 1.7.6 (c).
- Refer Fig. 1.7.6 (d). This is an address with proper network number and all 1s in the host field. This address allows machines to send broadcast packets to distant LANs anywhere in the Internet.
- If the address is "127.Anything" as shown in Fig. 1.7.6 (e) then it is a reserved address **loopback testing**. This feature is also used for debugging network software

1.7.4 Address Masks (Default Masks) :

- An address mask determines which portion of an IP address identifies the network and the host portion.
- The mask is represented by four octets. An octet is an 8-bit binary number equivalent to a decimal number in the range from 0 - 255.
- If a given bit of the mask is 1, the IP address is in the network portion of the address.
- If a given bit of the mask is 0, the IP address is in the host portion.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- For example consider a class C address 192.15.28.16. This is shown in Fig. 1.7.7 Note that 192.15.28 corresponds to the network part and 16 correspond to the host part.

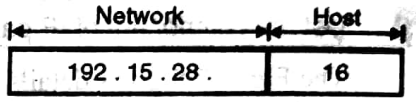


Fig. 1.7.7

- So as to differentiate the network and host parts. We have to use a mask 255.255.255.0.
- Table 1.7.1 shows the mask 255.255.255.0 in both decimal and binary form, aligned with the class C address 192.15.28.16, also in both decimal and binary form :

Table 1.7.1: IP address (In decimal and binary form)

Element	Network			Host
Mask	255	.255	.255	.0
	11111111	11111111	11111111	00000000
Address	192	.15	.28	.16
	11000000	00001111	00011100	00010000

- If a field of the network address is entirely used for the network number, than the mask has the decimal value 255 (binary 11111111)
- If an address field is entirely used for the host ID, than the mask has the decimal value 0.

Table 1.7.2

Decimal Value in Field of Mask	Binary Value in Field of Mask	Function
255	11111111	Identify network number
0	00000000	Identify host ID

- Accordingly, the address masks for the three network classes described above are as shown in Table 1.7.3. These masks are also called as default masks.

Table 1.7.3

Address Class	Address Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Which IP protocol version is being used currently ?

- The network protocol in the Internet is currently IPv4. It was first introduced in 1970's.
- After that the world of data communication has grown beyond imaginations. Even though IPv4 is a well designed protocol, it has some limitations.
- We need better addressing method for huge network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.7.5 IP Package :

Q. List the component of IP packages? Explain any one. MU - April 2013

The Fig. 1.7.8 gives details about IP package and the various components in it:

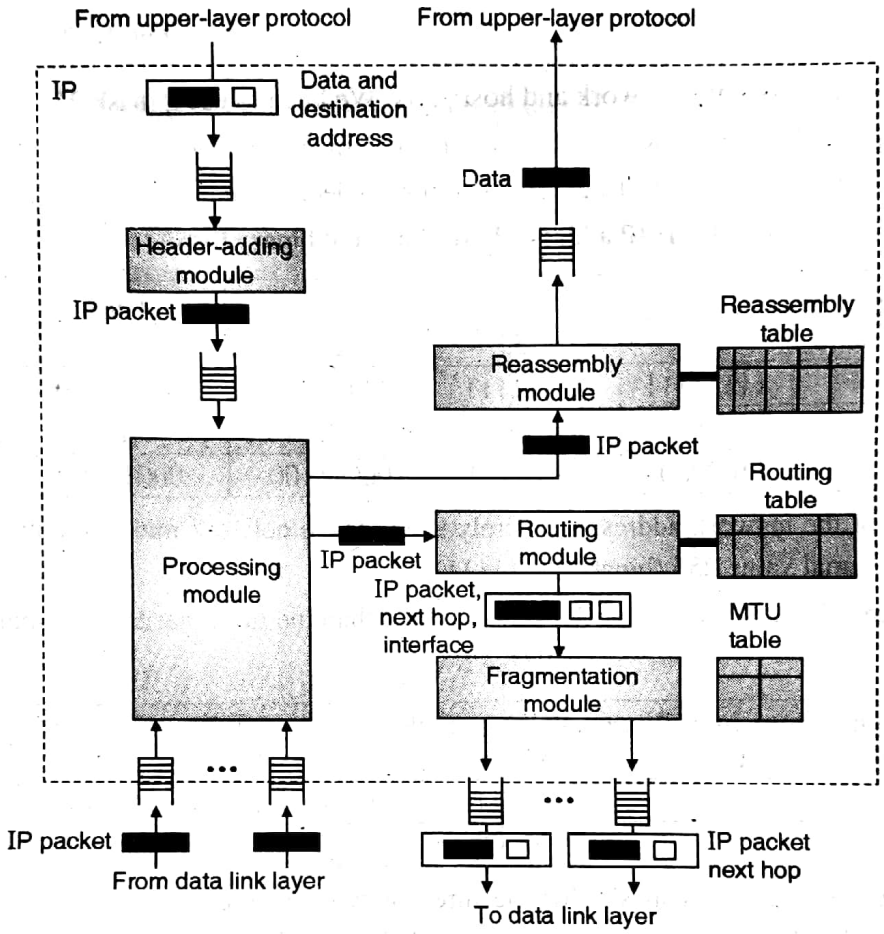


Fig. 1.7.8

Header-Adding Module :

The header-adding module of IP package receives data from an upper-layer protocol with the destination IP address mentioned in it. The module encapsulates the data in an IP datagram by adding the IP header.

Processing Module :

The processing module is the main component of the IP package. In our package, the processing module receives a datagram either from interface or from the header-adding module but it treats both cases in the same manner. A datagram is processed and routed regardless of from where comes.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

The processing module first checks whether datagram has reached its mentioned final destination.

- If yes than the packet is sent to the reassembly module.
- If the node is a router, it decrements it's time-to-live (TTL) field by one.
- If this value is less than or equal to zero(<= 0), the datagram is discarded and an ICMP message is sent to the original sender of packet.
- If the value of TTL is greater than zero (> 0) after decrement, the processing module sends the datagram to the forwarding module for further processing.

Routing (Forwarding) Module :

The routing i.e forwarding module collects an IP packet from the processing module as mentioned above. The packets which are needed to be forwarded are transferred in this component.

The forwarding module finds next hop(station) IP address can be final destination (if direct communication) or next router (if indirect communication) in the path to which packet should be forwarded. For this it takes help of routing table.

Forwarding module than sends the packet with the specific information to the fragmentation module.

Fragmentation Module :

The fragmentation module in IP package receives an IP datagram from the forwarding module. It gives the IP datagram, the IP address of the next hop also the interface number through which the datagram is sent out.

If datagram is of large size rather than the specified in MTU (Maximum Transfer Unit) fragmentation module fragments the datagram, adds a header to each fragment, and sends them to the ARP package for address resolution and delivery.

It uses MTU table for getting information related with MTU of particular datagram; which has only two columns specifies; Interface and MTU.

Reassembly Module :

The reassembly module receives those datagram fragments that have arrived at their final destinations which are forwarded from processing module.

In IP package, the reassembly module considers an unfragmented datagram as a datagram with only one fragment. There is no guarantee that the fragments arrive in order; since the IP protocol is a connectionless protocol.

The module uses a reassembly table with associated linked lists to to keep track of whether the fragments from one datagram can be intermixed with fragments from another

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

datagram. The reassembly module reassembles the all fragments which are belongs to the same datagram.

It keeps all records in reassembly table about the datagram which includes fields like: state, source IP address, datagram ID, time-out, and fragments. FREE or IN-USE are two values of the state field.

1.7.6 Limitations of IPv4 :

- The major limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-points on networks, and each networked node has a unique IP address.
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses for devices. Due to huge number of devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming limited, we may run out of IP addresses.
- If a network has slightly more number of hosts than a particular class, then it needs either two IP addresses of that class or the next class of IP address. A large number of host IP addresses are wasted.
- Other identified limitations of the IPv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng) was proposed.
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.
- The format and length of the IP addresses has been changed and the packet format also is changed.

1.8 IPv6

a) Introduction :

1. IPv6 is the recently revised form of the Internet Protocol (IP).
2. With ever increasing number of devices connected to the Internet, there is a need for large number of addresses than IPv4.
3. IPv6 will make use of 128-bit address.
4. It will allow near about 2^{128} addresses.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) IPv6 Header Format :

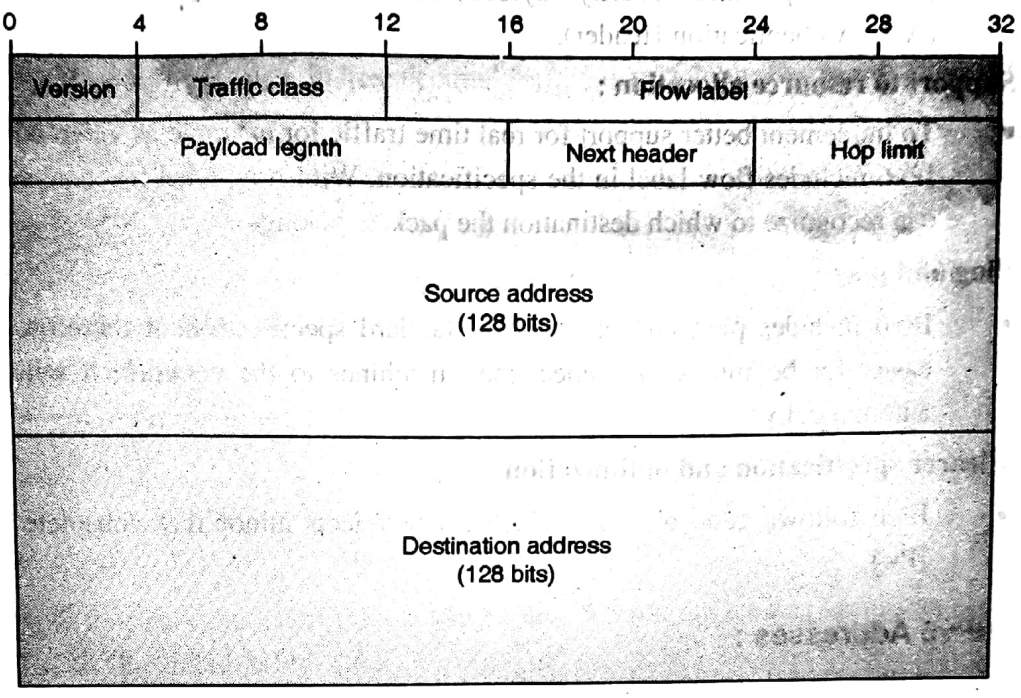


Fig. 1.8.1

c) Advantages of IPv6 :

1. Larger address space :

- IPv6 has 128-bit address space, which is 4 times wider in bits in compared to IPv4's 32-bit address space. So there is a huge increase in the address space.

2. Better header format :

- IPv6 uses a better header format. In its header format the options are separated from the base header.
- The options are inserted when needed, between the base header and upper layer data.
- The helps in speeding up the routing process.

3. New options :

- New options have been added in IPv6 to increase the functionality.

4. Possibility of extension :

- IPv6 has been designed in such a way that there is a possibility of extension of protocol if required.

5. More security :

- IPv6 includes security in the basic specification. It includes encryption of packets using

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH : Authentication Header).

6. **Support to resource allocation :**
   - To implement better support for real time traffic for example as video conference, IPv6 includes flow label in the specification. With flow label mechanism, routers can recognize to which destination the packets belongs.
7. **Plug and play :**
   - IPv6 includes plug and play in the standard specification. It therefore must be easier for beginners to connect their machines to the network, it will be done automatically.
8. **Clearer specification and optimization :**
   - IPv6 follows good observes of IPv4, and rejects minor flaws/obsolete items of IPv4.

1.8.1 IPv6 Addresses :

- An IPv6 address consists of 16 bytes (octets) i.e. it is 128 bits long as shown in Fig. 1.8.2

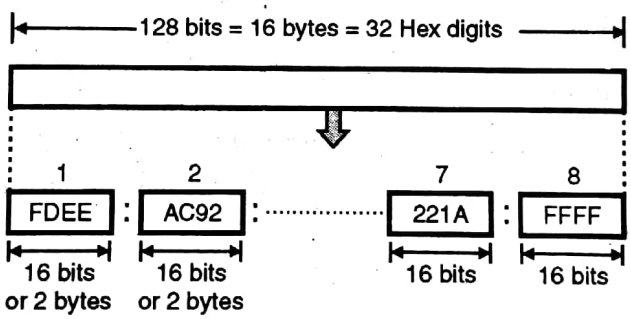


Fig. 1.8.2 : IPv6 address

Hexadecimal colon notation :

- IPv6 uses a special notation called hexadecimal colon notation. In this, the 128 bits are divided into 8 sections, each one is 2 bytes long.
- 2 bytes correspond to 16 bits. So in hexadecimal notation will require four hexadecimal digits.
- Hence the IPv6 address consists of 32 hex digits and every group of 4 digits is separated by a colon as shown in Fig. 1.8.2
- IPv6 uses 128-bit addresses. In this 15% of the address space is initially allocated, the remaining 85% being reserved for future use for expanding the address spaces of existing address types or for totally new uses.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1.8.2 Abbreviation :

- The IPv6 address, even in hexadecimal format is very long. But in this address there are many of the zero digits in it.
- In such a case, we can **abbreviate** the address. The leading zeros of a section (four digits between two colons) can be omitted.

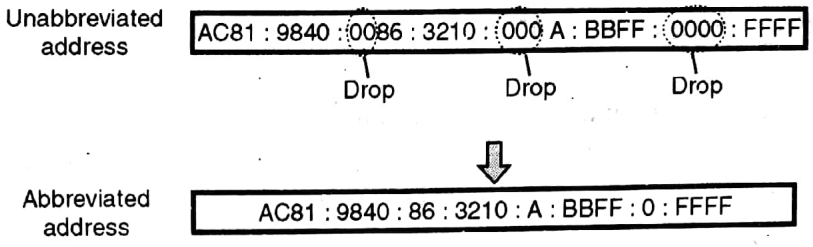


Fig. 1.8.3 : Abbreviated address

- Note that only the leading zeros can be dropped but the trailing zeros can not dropped. This is illustrated in Fig. 1.8.3

Further abbreviation :

- Further abbreviation are possible if there are consecutive sections consisting of only zeros.
- We can remove the zeros completely and replace them with double semicolon as shown in Fig. 1.8.4.

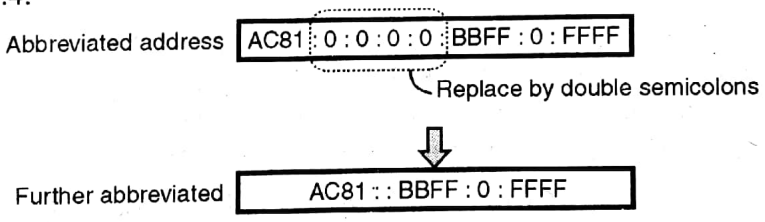


Fig. 1.8.4 : Further abbreviation

- It is important to note that abbreviation is allowed only once per address. Also note that if there are two runs of zero sections, then only one of them can be abbreviated.

Q. Show the unabbreviated colon hex notation for the following IPv6 addresses.

i. An address with 64 0's followed by 64 1's.

ii. An address with 128 0's.

iii. An address with 128 1's.

iv. An address with 128 alternative 1's and 0's.

v. An address with two alternate 1's and 0's. **MU - April 2013**

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

The solution is as follows :

1. 0000:0000:0000:0000:1111:1111:1111:1111
2. 0000:0000:0000:0000: 0000:0000:0000:0000
3. 1111:1111:1111:1111: 1111:1111:1111:1111
4. AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA
5. CCCC:CCCC:CCCC:CCCC:CCCC:CCCC:CCCC:CCCC

1.9 Migrating from IPv4 to IPv6

Since millions of computers and network endpoints (like printers, cameras, mobile sets, etc.) connected via the Internet for their day to day communication using Internet Protocol, or IP.

IP addresses are useful for identifying these network endpoints (computers, printers, cameras, mobile sets, etc.)

IPv4 addressing method was excellent, however, due to the unexpected expansion of the web , networking experts are facing problems.

The problems are like *insufficient addressing space* since at every second a new, 4th generation IP address is allocated, and according to estimates, we are going to face lack of addresses within 2 years.

Also it does not support *mobility* and *encryption.*

IPv6 was developed To solve these issues :

1. It was IPv4's success that made an upgrade necessary, which means that there is a significant installed base of users to upgrade. Keeping the transition orderly was a major objective of the entire IPng program, and there are no plans for a cutover date when IPv6 would be turned on and IPv4 turned off.
2. Hosts that upgrade to IPv6 will continue to exist as IPv4 hosts at the same time. It means deploy the IPv6 protocol stack in parallel with IPv4. In other words,
3. The hosts will continue to have 32-bit IPv4 addresses but will add 128-bit IPv6 addresses. By 1999, hundreds of networks were linked to the 6bone.
4. The transition can be achieved through three strategies given by IETF: *protocol tunneling*, IPv4/*IPv6 dual stack and header translation.*

Q. Explain the transition strategies from IPv4 to IPv6 MU - April 2013

Because of the enormous number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen easily.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

It will take a large amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems. Three strategies have been devised by the IETF to help the transition.

Dual Stack :

Till the all address are getting migrated network nodes should use Dual stack of IPv4 and IPv6. To decide which version to use when sending a packet to a destination, the source host queries the DNS. If DNS returns:

- IPv4 address, the source host sends an IPv4 packet.
- IPv6 address, the source host sends an IPv6 packet

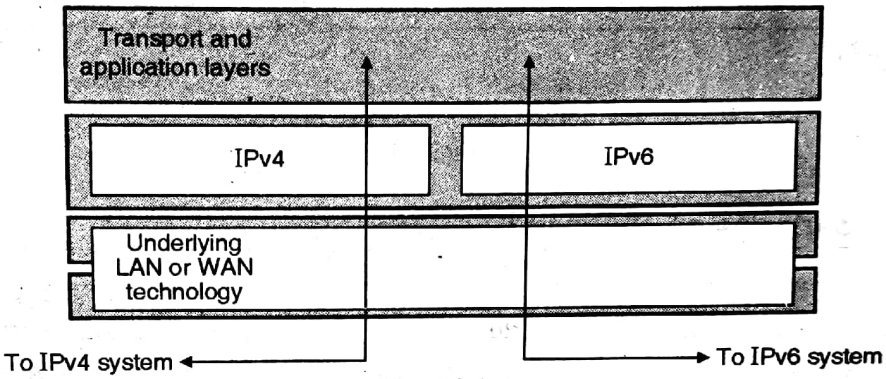


Fig. 1.9.1

Tunneling :

In this strategy is useful when; two computers wants to communicate with each other using IPv6 but while transferring packet over the network it will go through the nodes which are using IPv4.

In this case the IPv6 packet will be encapsulated in IPv4 packet and forwarded over the IPv4 region; while going out of than region the packet will be decapsulated and it will be an IPv6 packet for the destination. It gives feel of IPv6 packet is going through tunnel made up of IPv4 packet.

The protocol value is set to 41, since an IPv4 packet is carrying an IPv6 packet as data.

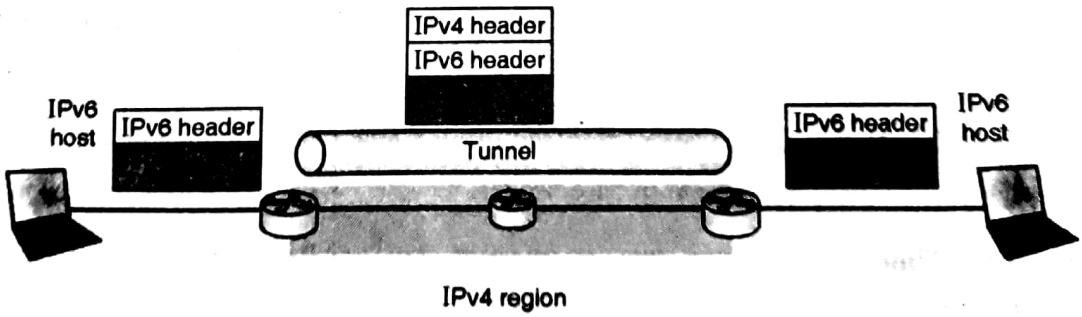


Fig. 1.9.2

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Header Translation :

When the majority of the Internet has moved to IPv6 but some systems still use IPv4 the header translation strategy is needed.

The nodes which are using IPv4 will not able to understand the IPv6 hence the format of IPv6 is totally changed using mapping method. Some rules used in transforming an IPv6 packet header to an IPv4 packet header.

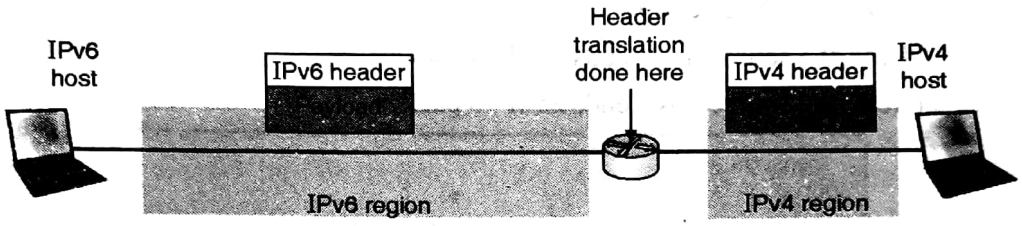


Fig. 1.9.3

1.10 comparisons of IPv4 and IPv6 Headers

Q. Differentiate between IPv4 and IPv6. **MU - April 2013**

Sr.	Parameter	IPv4 Header	IPv6 Header
1.	**HLEN**	options and padding fields (It is multiple of 32 bits)	Length of header fixed In this version it is 320 bits.
2.	**Service Type**	Number of fields total are 14 field Service type field - contain a) Precede nee b) type of service c) MBZ (must be zero) (TL)	Label together take over the Function of service type. Number of fields are 8 only.
3.	**Total Length**	Total length of packet is 16 bit field so IPv4 Packet is, 2^{16} = 65,535 long bytes.	Replaced by payload length field which give total length of extension needs + user data
4.	**Identification**	Identification, flag and offset fields are present in base header.	Are eliminated and included in Fragmentation extension header.
5.	**TTL(Time to leave)**	Time to live in seconds For a packet on internet.	Replaced by Hop limit field Same (HL)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sr.	Parameter	IPv4 Header	IPv6 Header
6.	**Protocol**	Protocol field used to create user Data (P)	Replaced by next header field (NH)
7.	**Header Check sum**	Header checksum is provided to calculate checksum in header.	Eliminated because the checksum is provided by upper Larger protocols.
8.	**Options**	Options fields are present in header.	Implemented as extension headers in IPvng (next generation)
10.	**Address size**	Source and destination address are 32 bits each	Source and destination address are 128 bits each

Review Questions

Q. 1 What are computer networks? Why it is required.

Q. 2 What are computer networks? Why it is required.

Q. 3 What are various networking standards used.

Q. 4 Explain how OSI model exchanges data between various layers

Q. 5 Explain functionality of each layer in OSI model.

Q. 6 Describe the functionality of each layer in TCP/IP protocol model.

Q. 7 Give advantages and disadvantages of OSI model.

Q. 8 Compare OSI model with TCP/IP protocol suite.

Q. 9 Explain the presentation layer and its functions in details.

Q. 10 Explain the data link layer and its functions in details.

Q. 11 Explain the network layer and its functions in details.

Q. 12 Explain the presentation layer and its functions in details.

Q. 13 Give functionality of each layer in TCP/IP protocol model.

Q. 14 Write a short note

a) IPv4 b) IPv6

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Q. 15 Compare and contrast between IPv4 and IPv6.

Q. 16 Explain header format of IPv4.

Q. 17 Describe header format of IPv6.

1.11 University Questions and Answers

April 2013

Q. 1 Show the unabbreviated colon hex notation for the following IPv6 addresses. **(Section 1.8.2)** **(5 Marks)**

i. An address with 64 0's followed by 64 1's.
ii. An address with 128 0's.
iii. An address with 128 1's.
iv. An address with 128 alternative 1's and 0's.
v. An address with two alternate 1's and 0's

Q. 2 Find the netid of the following IP addresses : **(Section 1.7.2)** **(5 Marks)**

i) 114.34.2.8 ii) 132.56.8.6
iii) 208.34.54.12 iv) 251.34.98.5
v) 129.14.6.8

Q. 3 Explain the transition strategies from IPv4 to IPv6. **(Section 1.9)** **(5 Marks)**

Q. 4 Find the error, if any, in the following IPv4 addresses **(Section 1.7)** **(5 Marks)**

i. 127.045.112.27 ii. 12.24.35.7.8
iii. 10110011.23.45.234 iv. 76.27.256.23
v. A23.56.78.5

Q. 5 Differentiate between IPv4 and IPv6. **(Section 1.10)** **(5 Marks)**

Q. 6 List the component of IP packages ? Explain any one **(Section 1.7.5)** **(5 Marks)**

Q. 7 Describe the function of the transport layer in the OSI model. **(Section 1.3.2(4))** **(5 Marks)**

Q. 8 Explain Stop-and-wait Protocol and Go-Back-N Protocol in the transport layer. **(Section 1.4.1 (3))** **(5 Marks)**

❑❑❑

www.MumbaiBScITStudy.Com

MumbaiBScITStudy

CHAPTER 2

Network Layer

Syllabus

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol Version 4 (ICMPv4)
- Mobile IP

2.1 ARP (Address Resolution Protocol)

1. Introduction :

- An internet is consists of various physical networks connected together using routers and other internetworking devices.
- Any packet of data started from host which may be passed onto many physical networks before reaching to final destination.
- At network layer host and router are identified by logical address.
- At physical level host and routers are identified by physical address.

2. Logical Address :

- Logical address is called as IP address in TCP/ IP protocol suit.
- Logical address is 32 bits long and it is implemented using software.
- Logical address is set by the operating system of machine.
- The hosts and routers are differentiated at Network layer by using logical address of machine.
- Ex. 192.168.0.23

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3. Physical Address :

- Physical address is also called as MAC address.
- Physical address is 48 bits long and it is set by manufacturer.
- It will be unique for any network or LAN.
- The host and routers are uniquely identified by using physical address at physical layer.
- It is local address and it is implemented in hardware.
- Ex. B4:6B:A4:69:73:BA

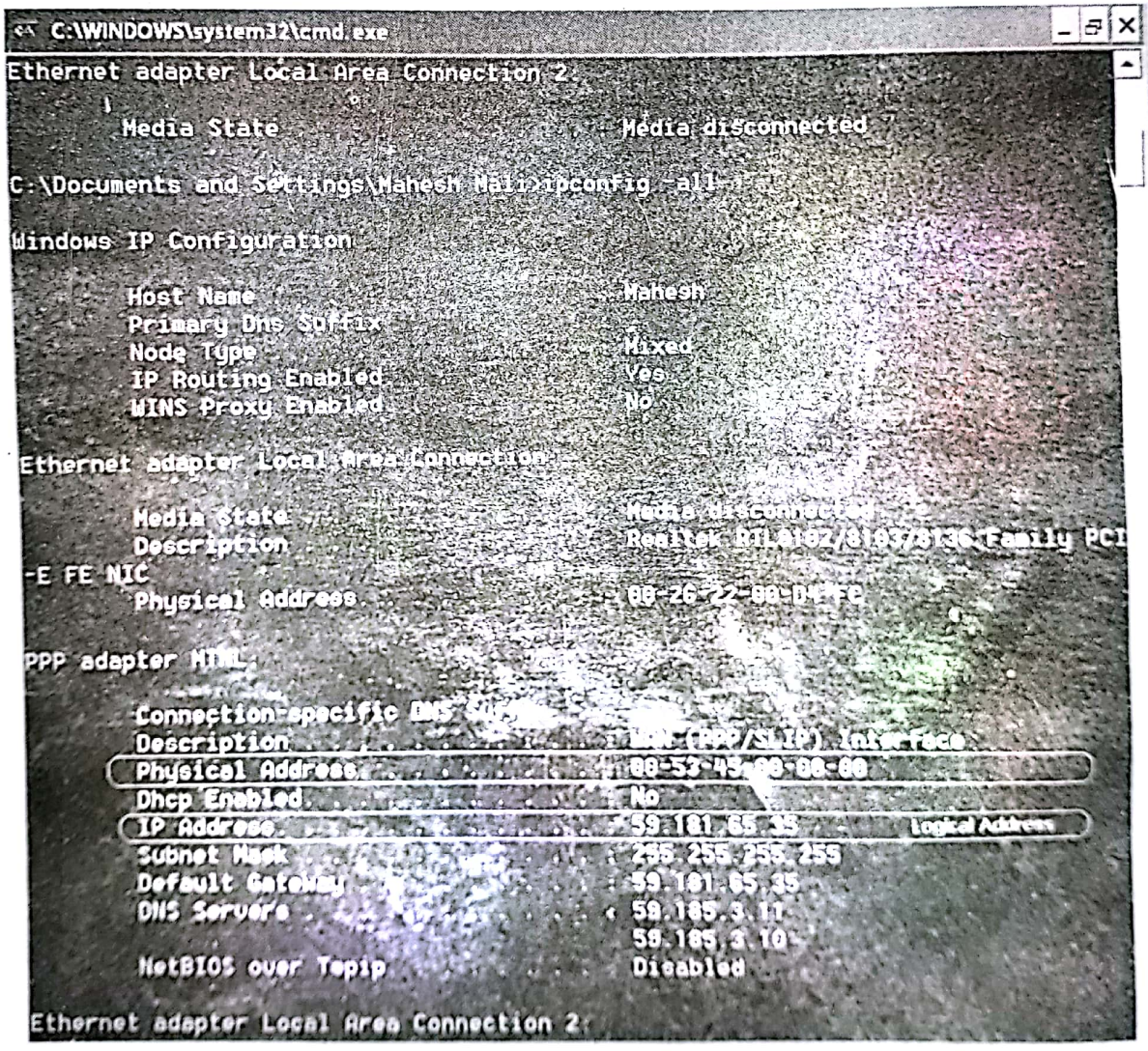


Fig. 2.1.1 : Logical and Physical address of network

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4. Comparison :

- The physical address and logical address are two different identifiers.
- They are used in delivery of packet.

5. Mapping :

- All host or router requires mapping of logical address to physical address and vice versa.

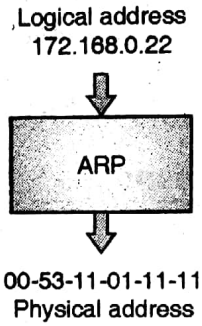


Fig. 2.1.2 : Address mapping using ARP

- This mapping can be done using two ways :

(1) Static mapping :

- In this technique we create a table which associates logical address with the physical address.
- Like IP address table in local machine.
- Drawbacks
  - Physical address may change on changing NIC of machine
  - Physical address may change on changing location of machine
  - Even address changes on computer power on and off.

(2) Dynamic mapping :

- Machine knows one of the addresses of other machine only and it can use a protocol to find the other addresses.
- Uses protocol to map logical address to physical address and vice versa.
- This technique is used for ARP and RARP.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Fig. 2.1.3 : Address mapping in RARP

2.2 ARP Request and ARP Response

1. Introduction :

- Address Resolution Protocol is used to maps logical address to physical address (i.e. IP address to MAC Address)
- At any point of time it will get MAC address of host or router which has an IP datagram to send to another host or router.
- ARP maps logical address of required node and we require physical address of that node.

2. Process of mapping address :

- When system A wants physical address of machine with logical address 192.168.0.22
- **Phase I : Request Message is broadcasted**

a) System A generates the request of physical address of machine with logical address 192.168.0.22

b) Request message will go, to machine X situated next to it.

c) X realizes that this is an ARP request, if destination IP not matching with its own IP address forward same to Y.

d) Y will check the ARP request since the destination MAC is all ones and it will check for destination IP. If it doesn't matched the request will be forward, to machine Z where the destination IP address will be matched.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

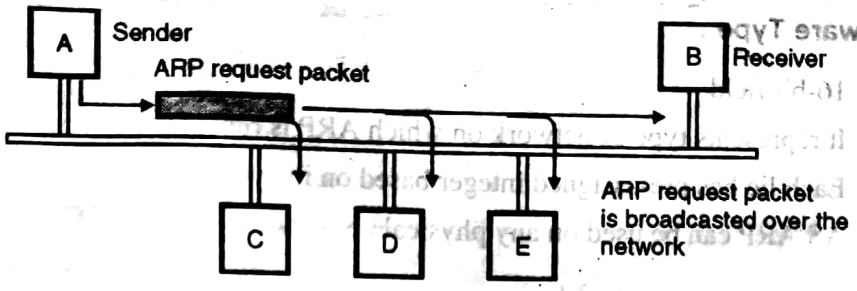


Fig. 2.2.1 : ARP request is broadcast

- **Phase II : Reply Message is Unicasted**
  - a) If destination IP matches with any machines IP address it will send reply.
  - b) The reply packet will be unicasted (sent to only one machine) directly to source by filling up destination physical address.
  - c) Therefore the reply packet is Unicast in nature.

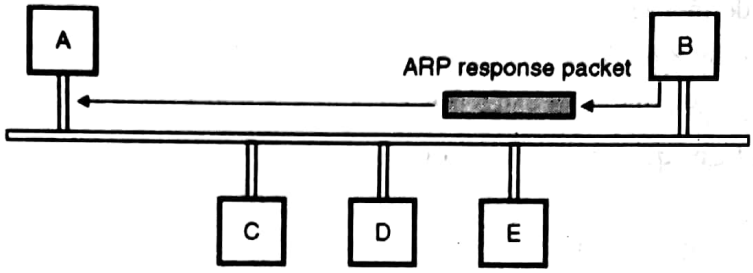


Fig. 2.2.2 : ARP response unicast

2.3 ARP Packet Format

Hardware Type (16 Bits)		Protocol Type (16 Bits)
Hardware Length (8 Bits)	Protocol Length (8 Bits)	Operation (Request 1, response 2) (16 Bits)
Sender Physical Address (32 Bits)		
Sender Logical Address (32 Bits)		
Receiver Physical Address (32 Bits)		
Receiver Logical Address (32 Bits)		

Fig. 2.3.1 : ARP packet Format

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

1. **Hardware Type :**
   - 16-bit field
   - It represents type of network on which ARP is running.
   - Each lie has pre-assigned integer based on its type.
   - AS ARP can be used on any physical network.
   - E.g. For Ethernet it is 1.
2. **Protocol Type :**
   - This indicates the type of protocol used.
   - It is a 16 bit field
   - e.g.IPV4 the field will be 0800_{16}
3. **Hardware Length :**
   - It defines length of physical address in bytes.
   - It is an 8 bit field.
   - E.g. Ethernet field value is 6.
4. **Protocol Length :**
   - It defines length of logical address in bytes.
   - It is a 8 bit field.
   - E.g. for IPV4 the value is 4.
5. **Operation :**
   - The operation indicates type of ARP packet.
   - Request value is 1 and for reply value is 2.
6. **SHA (Sender physical Address) :**
   - This is a variable length fields
   - It defines source physical address.
   - For Ethernet the size of field is 6 byte
7. **SPA (Sender protocol Address) :**
   - This is a variable length fields
   - It defines source logical address.
   - For IP the size of field is 4 byte
8. **DHA (Destination physical Address) :**
   - This is a variable length fields
   - It defines physical address of destination or target machine.
   - For Ethernet the size of field is 6 byte

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

9. DPA (Destination protocol Address) :

- This is a variable length fields.
- It defines logical address of destination or target machine.
- For IP the size of field is 4 byte

2.4 ARP Encapsulation

1. ARP package is encapsulated in a data link frame.
2. These packets are used to send over the network when it reaches to target host
3. Then it will open by target to access its contains.

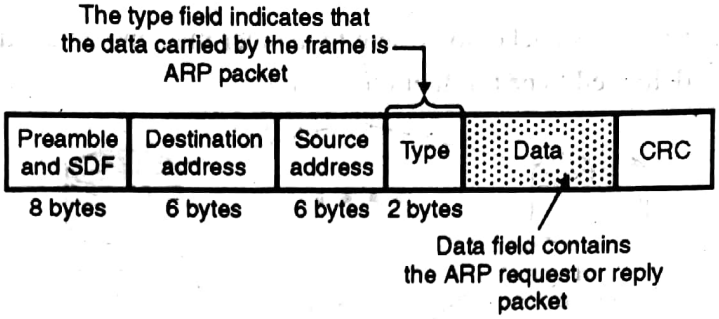


Fig. 2.4.1 : Encapsulation of ARP packet

2.5 ARP Operations

1. Introduction :

- The functioning of typical ARP on internet will be as follows,
- As Sender knows IP address of Machine B and want to retrieve physical address to send packets to Receiver,
  - a) Sender wants to send a packet to B, but Sender only knows Receiver's IP address
  - b) Sender broadcasts ARP request with Receiver's IP address
  - c) All machines on the local network receive the broadcast message.
  - d) Receiver replies with its own physical address
  - e. Sender adds Receiver's address information to its IP table
  - f. Sender delivers packet directly to Receiver.

2. Cases of ARP :

a) Sender wants to send packet to another machine on same network

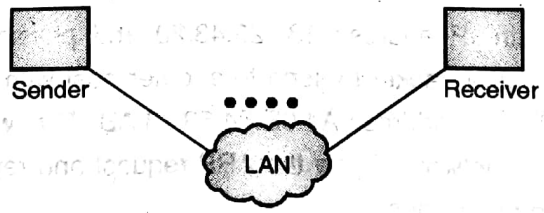


Fig. 2.5.1 : Sender and receiver both located in same network

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) Sender wants to send packet to another machine on another network then packet is first delivered to another router.

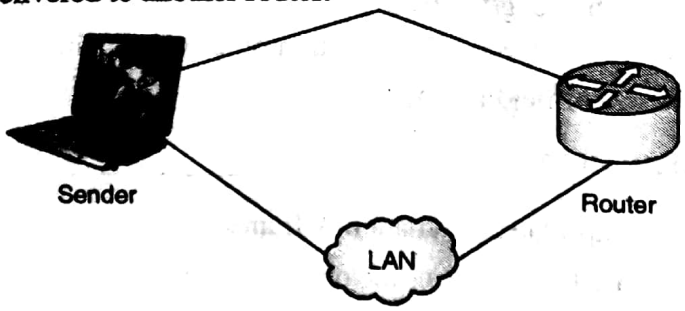


Fig. 2.5.2 : Sender sends data to router

c) A router receives packet to be sent to another machine on another network it will be first delivered to next router on its path.

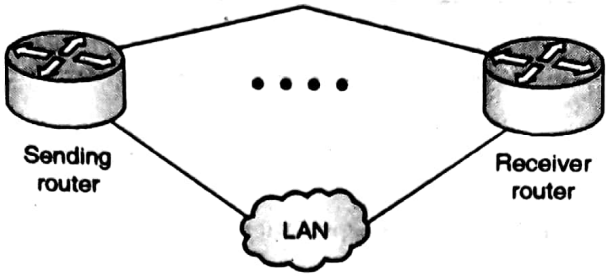


Fig. 2.5.3 : Sending packet from one network to other network

d) A router gets packet to be sent to machine on same network

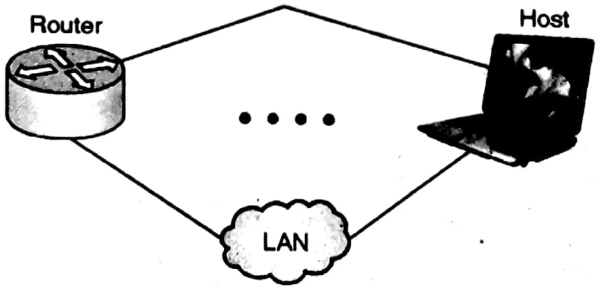


Fig. 2.5.4 : Receiver receives packet from other network

2.6 ARP Solved examples

Example 2.6.1 : Host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Soln. :

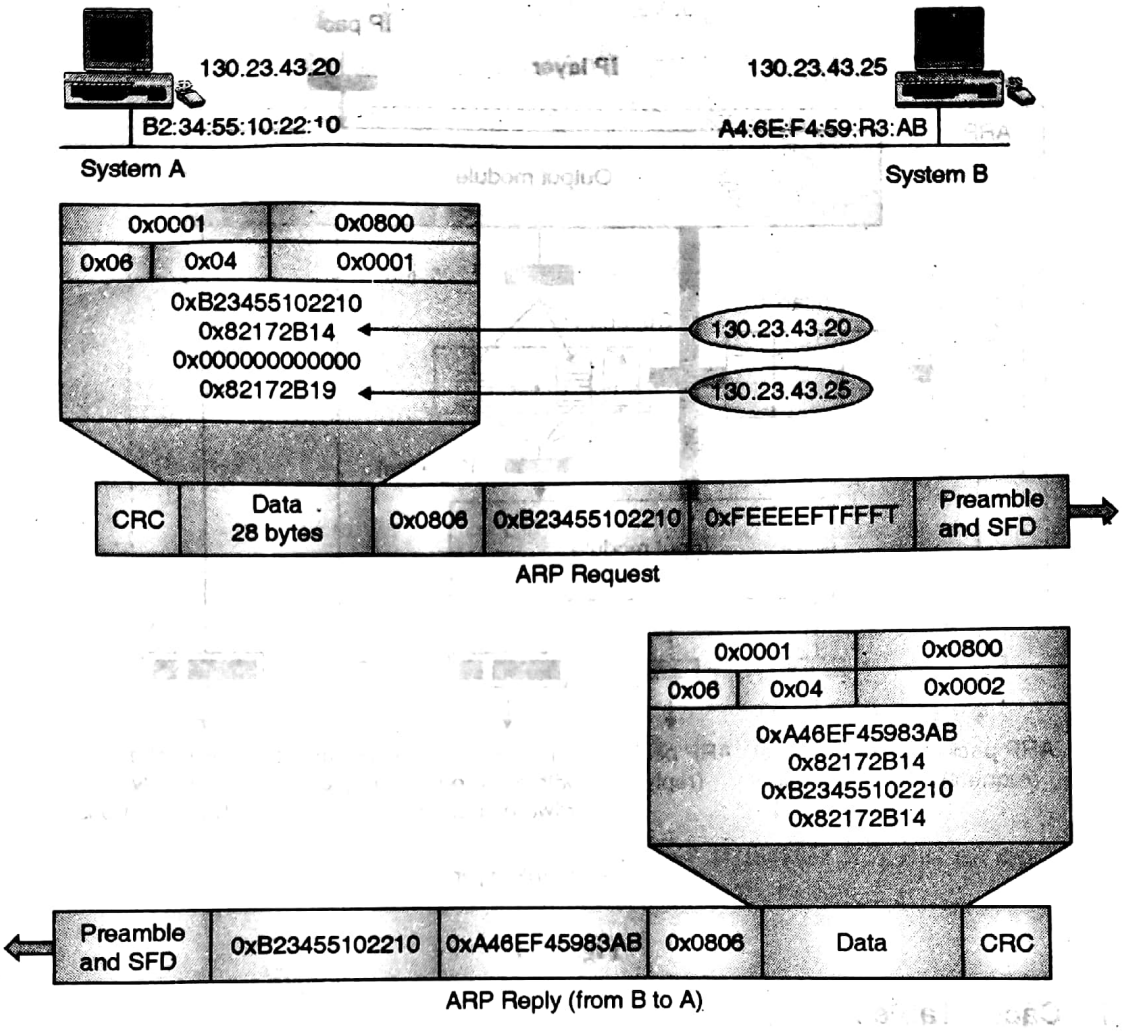


Fig. P. 2.6.1

2.7 ARP Package

Introduction :

- The hypothetical model for ARP processing can be represented as shown in Fig. 2.7.1.
- This package will receive the IP datagram which have the logical address and requires the physical address of destination machine.
- There are five important modules of ARP Package :
  - Cache Table
  - Queue
  - Output module
  - Input module
  - Cache control module

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

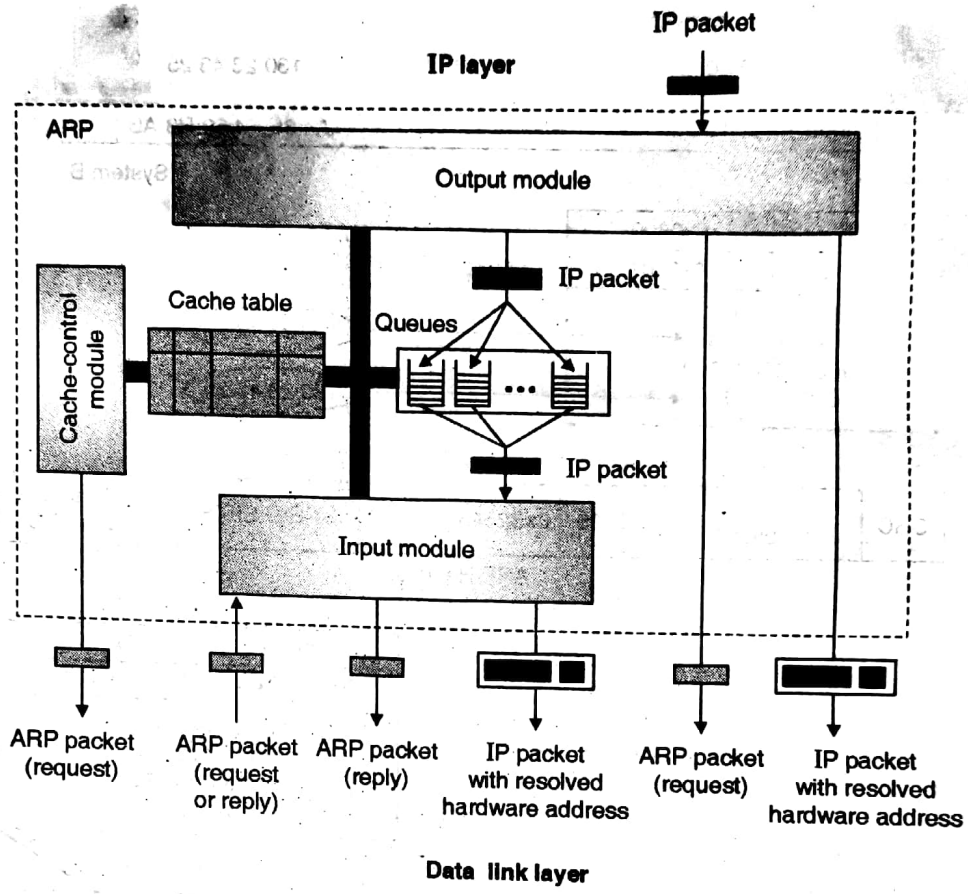


Fig. 2.7.1

2.7.1 Cache Table :

- Any Sender needs to send many *IP* datagram to same destination.
- It is not good to use ARP protocol for each IP datagram and hence cache table is used.
- The physical address received due to ARP reply is stored in cache table and can be used by other IP datagram for same destination in future.
- As size of cache table cannot exceeds above certain limit, we need to remove some entries which will not be used in future since we cannot keep all the entries for unlimited time.
- The cache table has following entries :

1. **State :**

   - There can be three different States of any entry in cache table available as explained below :

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

a) Free
   - The time to leave (TTL) for this entry is expired
   - This space can be utilized for a new entry,

b) Pending
   - The request is sent for this entry.
   - But, reply has not yet been received so it is in pending state.

c) Resolved
   - Entry is complete
   - IP datagram along with hardware address is sent to data link layer.

2. Timeout :

- This column is used to indicate the life time of entries.
- It is stored in number of seconds.

3. Queue :

- Many Queues are used for ARP.
- Packets waiting for physical address are stored in Queues

4. Attempts :

- This field shows number of times ARP request is sent out for this entry of cache table.

E.g.

State	Queue	Attempt	Timeout	Protocol	H/w Address

2.7.2 Queue :

- ARP package offers a set of queues for individual destination.
- The queue holds the IP packets as ARP tries to determine the hardware address.
- The output module keeps unresolved IP packets into the corresponding queue.
- Input module resolves physical address of IP packets from queue and transfers it to data link layer for further communication.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2.7.3 Output Module :

- Output module is used to wait for IP packet from network layer.
- This will checks the cache table to find entry for incoming packets if the entry is found
  1. If entry in table is found but state is *resolved* the packet along with destination hardware address is passed to data link layer for transmission,
  2. If entry in table is found but state is *pending* then the packet is put into the Queue.

2.7.4 Input Module :

Q. Explain the Input module of ARP. MU - April 2013

- Input module waits until an ARP packet (i.e request or reply) appear.
- Input module checks entry of corresponding ARP packet in the cache table; If entry is found
  1. If entry in table is found but state is *pending* than one by one unresolved packet is dequeue.
  2. After resolving; IP packets are forwarded to data link layer with their hardware addresses. Then entry in table is updated as *resolved.*
  3. If entry in table is not found, the module creates new entry and updates it in the cache table.
  4. As ARP Request is asked; Immediately ARP Reply packet is created by changing the value of operation field from request to reply and filling the target hardware address.

2.8 The Reverse Address Resolution Protocol (RARP)

1. Introduction :

- An internet is consists of various physical networks connected together using routers and other internetworking devices.
- ARP is used for solving the problem of finding out which hardware address corresponds to a given logical or IP address.
- Some times we face a reverse problem i.e. we have to find logical (IP) address of corresponding to hardware address which can be solved by using RARP (reverse address resolution protocol).

2. Working :

- An internet is consists of various physical networks connected together.
- The newly added computer is allowed to broadcast its Ethernet (hardware) address.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The RARP server looks at this request, then it looks up the Ethernet address in its configuration files and sends back the corresponding IP address.
- Using RARP is actually better than embedding an IP address in the memory image because it allows the same image to be used on all machines.

Hardware type		Protocol type
Hardware address length	Protocol address length	Opcode
Source hardware address :::		
Source protocol address :::		
Destination hardware address :::		
Destination protocol address :::		

Fig. 2.8.1 : RARP Header

3. Disadvantages :

- RARP uses a destination address of all 1s (means limited broadcasting) to reach the RARP server. Such broadcasts are not forwarded by routers, so a RARP server is needed on each network.
- To solve above problem, another bootstrap protocol called BOOTP has been invented.

2.9 ICMP (Internet Control Message Protocol)

1. Introduction :

- As we know that IP provides unreliable and connectionless datagram delivery of datagram from its original source to its final destination.
- It was designed this way to make efficient use of network resources.

2. Drawbacks of IP :

- Lack of error control
- No mechanism for detecting or correcting the error
- Lack of any assistance mechanisms.
- No mechanism for host and management queries

3. Working :

- The Internet Control Message Protocol reports all errors and sends control messages on behalf of IP (Internet protocol).

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- ICMP does not attempt to report errors and provide feedback on specific conditions. ICMP messages are carried similar to IP packets and are therefore unreliable.
- A host sometimes needs to determine if a router (or another host computer) is alive or not.
- Sometimes a network manager needs information from another host computer or router.
- The Internet Control Message Protocol (ICMP) is works with IP.
- ICMP is a network layer protocol.
- ICMP messages are not directly passed to the data link layer as expected.
- The messages to be sent is first encapsulated inside IP datagram.

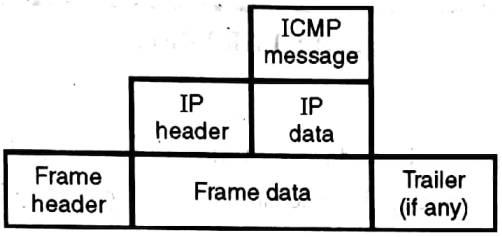


Fig. 2.9.1 : ICMP encapsulation

- Ping will posts an ICMP echo request message in a datagram and sends it to a selected destination. The user chooses the destination by specifying its IP address or name on the command line in a form such as :

  ping 100.50.25.1

- Once the destination receives the echo request message, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times.
- If no answer arrives, ping indicates that the destination is unreachable.

2.9.1 Types of Messages :

Q. Explain the source quench message and time exceeded message in ICMPv4 .

MU - April 2013

- ICMP messages are broadly divided into two categories as :
  1. Error reporting messages
  2. Query messages.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Error reporting messages :

- ICMP is mainly used for error reporting.
- ICMP does not correct the errors.
- Error correction is left to the higher level protocols.
- ICMP always sends the error reporting messages to the original source.

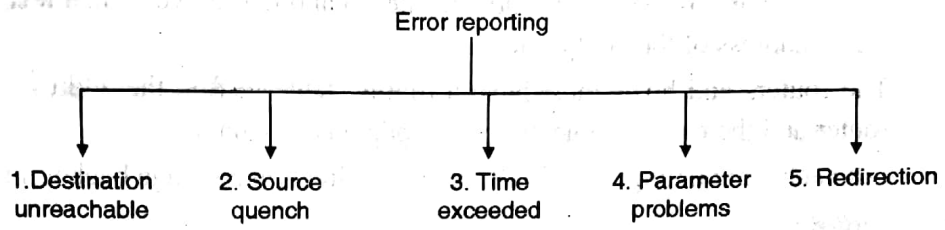


Fig. 2.9.2 : Error reporting messages

a) Destination unreachable :

- A router cannot forward or deliver an IP packet, it sends a destination unreachable ICMP message back to the original source.

b) Source quench message :

- A router or host computer uses this message to report congestion to the original source and to request it to reduce its current rate of packet transmission.
- Source quench message is ICMP is designed to add a kind of flow control and congestion control to IP.
- This message serves two purposes :
  1. It tells the source that the datagram has been discarded
  2. It gives a warning to the source that the source should slow down (quench) because congestion has taken place somewhere.

c) Time exceeded message :

Q. Explain the use of time exceeded message of ICMP. MU - April 2013

- This message is generated in two different cases as given below :
  1. TTL = 0
     - Datagram discarded and send a time exceeded message back to the original source.
  2. If all the fragments which make up a message do not arrive at the destination host within a certain time limit then time exceeded message is sent back.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

d) Parameter problem message :

If a router or destination host finds some ambiguity or missing value in any of the field of the datagram then it needs to discard such datagram and sends the parameter problem message back to the source.

e) Redirection message :

- If a router or host wants to send a packet to another network then it should know the IP address of the next router.
- The routers and hosts must have a routing table to find the address of the next router and the routing table has to be updated constantly.
- For such an updating, the ICMP sends a redirection message back to its host.

Query messages :

- The ICMP can diagnose some of the network problems through the query messages.
- The query message is a group of four different pairs of messages,

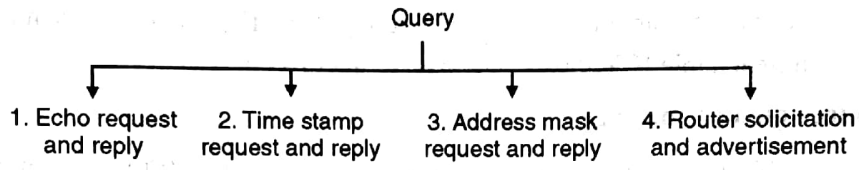


Fig. 2.9.3 : Query messages

a) Echo request and reply :

- This is a pair of two messages designed for diagnosis purpose.
- Messages determine whether two systems (hosts or routers) can communicate with each other.

b) Time stamp request and reply :

- This pair of messages used by the hosts and routers to determine the round trip time needed for an IP datagram to travel between them.
- It can also be used for synchronizing the clocks in two machines (hosts or routers).

c) Address mask request and reply :

- A host may know its full IP address but may not know its bifurcation.
- So it can send an address mask request message to the router. The router then sends back the address mask reply message.

d) Router solicitation and advertisement :

- A host that wants to send data to a host on another network must know the address of routers connected to its own network.
- In such situations the router solicitation and advertisement messages can help.

www.MumbaiBScITStudy.Com

MumbaiB.Sc.IT Study

- A host can broadcast a router solicitation message or multicast same message.
- The routers receiving this message can broadcast their routing information using the router advertisement message.

2.10 Mobile IP

1. Introduction :

- An internet is consists of various physical networks connected together using routers and other internetworking devices.
- Many internet users have portable computers like laptops and they want to stay connected to the internet even when they are outside and moving.
- The existing IP addressing system can not work properly for mobile users.

2. Addressing :

- Problem is the addressing scheme itself as host computer are continuously changing location,
- Types of Host computers

i. Stationary Host :

1. IP address is assigned by assuming that computer is at specific location on network.
2. If network changes such addresses are no longer valid. Such scheme is called stationary host.

ii. Mobile Host :

1. When computer hosts are moving from network to network then IP address needs to be modified.
2. For implementing scheme we can use one of many available solutions,
3. Changing address
   - i. We can change the address as it goes from one network to other network.
   - ii. Host will make use of DHCP server for getting new address on new network.
   - iii. In this case configuration files and DNS table needs to be updated.

iii. Two addresses :

i. Each host will have two addresses one address to be used at home network called home address and other address is used in other foreign networks called as care of address.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

ii. Home address is permanent while care of address is temporary and changes when computer move from one network to other network.

3. Agents :

- The address changes should be visible to entire network which is done with help of home agent and foreign agents.
- **Home Agent :**
  - i. It is a router attached to home network of mobile host.
  - ii. Home agent sends packets to foreign agents.
  - iii. Every site which has to allow the users to roam has to create a home agent.
- **Foreign Agent :**
  - i. It is a router attached to foreign network.
  - ii. Every site which has to visitors has to create a foreign agent.
  - iii. When a mobile host shows up at a foreign site it contacts the foreign host there and registers itself.
  - iv. The foreign host then contacts the user's home agent to give him a care-of-address which is normally the foreign agent's own IP address.
  - v. When mobile host acting like a foreign agent, the care of address called as collocated address.

4. Working phases :

Q. What are the three phases that a mobile host should go through to communicate with the remote host? **MU - April 2013**

OR

Q. Describe 3 phase of communication between remote host and mobiles host. **MU - April 2013**

- The mobile IP performs its functions in three different phase as below :
  1. Discover the Agent
  2. Agent registration
  3. Data transfer
- Discover Agent
  - First mobile host discover the home agent before leaving home network.
  - A mobile host then search for foreign agent after reaching to foreign network.
  - This address discovery have two type of messages.

www.MumbaiBScITStudy.Com

MumbaiB.Sc.IT Study

Agent advertisement

Router advertises using ICMP advertisement about its existence to packet if it works as agent.

Agent Solicitation

If host has changed location to new network not yet received agent advertisement then it will initiates agent solicitation.

Agent Registration

- Once mobile host moved to foreign network and discovered by foreign by foreign agent then needs to register itself on that network.
- To register with foreign network a request message will be sent to foreign agent to register its care of address who will approve and sends reply message.

Data Transfer

- After agent discovery and registration mobile host can communicate with otrher host with new care of address.
- If static sending host wants to send message to mobile receiving host the communication will takes place in following steps,

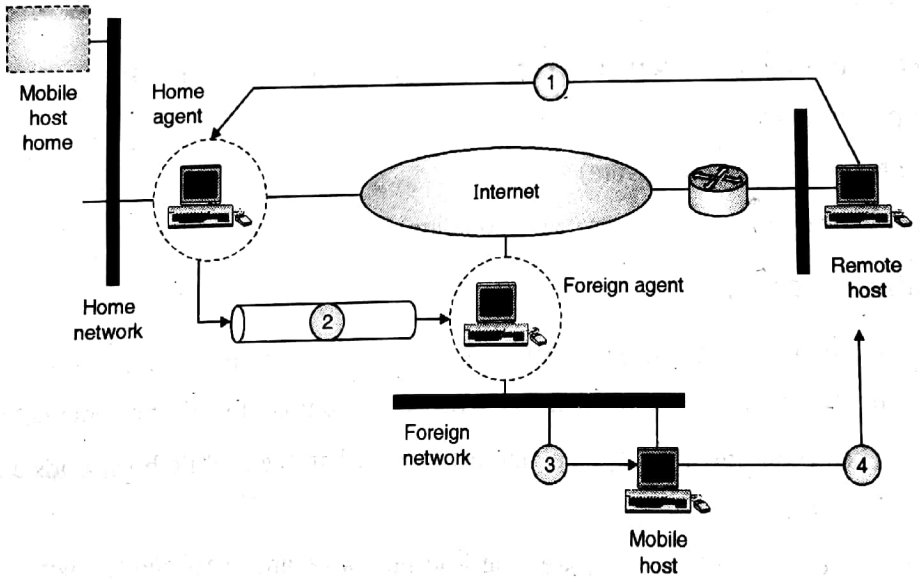


Fig. 2.10.1 : Mobile IP communication

a) communication from sending host to home agent

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) communication from home agent to foreign agent

c) communication from foreign agent to receiving host

d) communication from sending host to sending host

- When a packet arrives at the user's home LAN it comes in at some router which is attached to the LAN.
- The router then locates the host by broadcasting an ARP packet asking the Ethernet address.
- The home agent answers this question by giving its own Ethernet address.
- Then router sends the packet to the home agent.
- It then sends the packet toward the care-of-address by encapsulating it in the payload field of an IP packet addressed to the foreign agent.
- The foreign agent wants to remove encapsulation of data and delivers them to the data link address of the mobile host.
- The home agent offers the care of address to the sender so that future packets can be tunnelled directly to the foreign agent.

2.11 Inefficiency In Mobile IP

Q. What is the inefficiency in mobile IP? Give Solution for it. MU - April 2013

- There is possibility of inefficient communication involving mobile IP

The two types of inefficiency are involved :

1. Double crossing or 2X (severe)
2. Triangle routing or dog-leg routing (moderate)

1. Double Crossing :

- Double crossing occurs when a remote host tries to communicate with a mobile host and the mobile host has been moved as remote host in the same network.
- The communication is local and efficient; when the mobile host sends a packet to the remote host.
- However; the packet crosses the Internet twice and inefficient; when the remote host sends a packet to the mobile host.
- Since computers usually communicates with the other local computers the inefficiency from double crossing is considerable.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

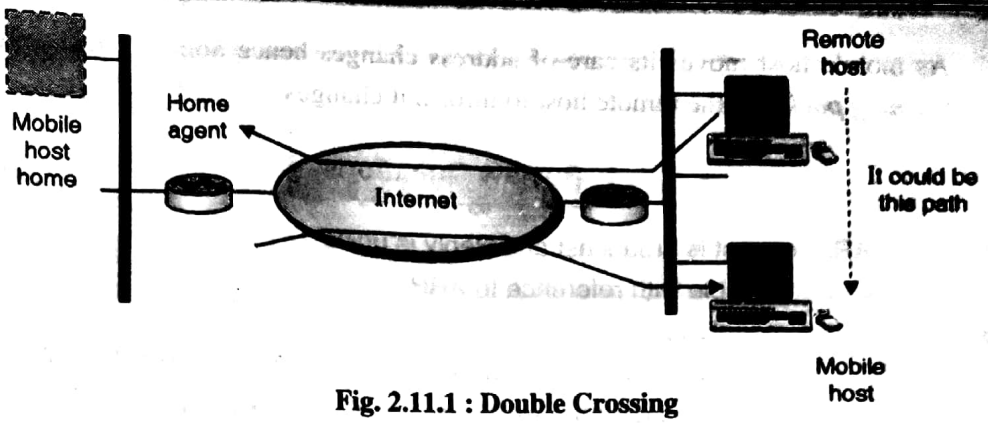


Fig. 2.11.1 : Double Crossing

2. Triangle Routing :

- Triangle routing occurs when the *remote host* communicates with a *mobile host* that is not attached to the same network as the mobile host.
- There is no inefficiency; when the mobile host sends a packet to the remote host.
- When the remote host sends a packet to the mobile host;

Firstly the packet goes from the remote host to the home agent and then to the mobile host and than the packet travels *the two sides of a triangle* as shown in the Fig. 2.11.2.

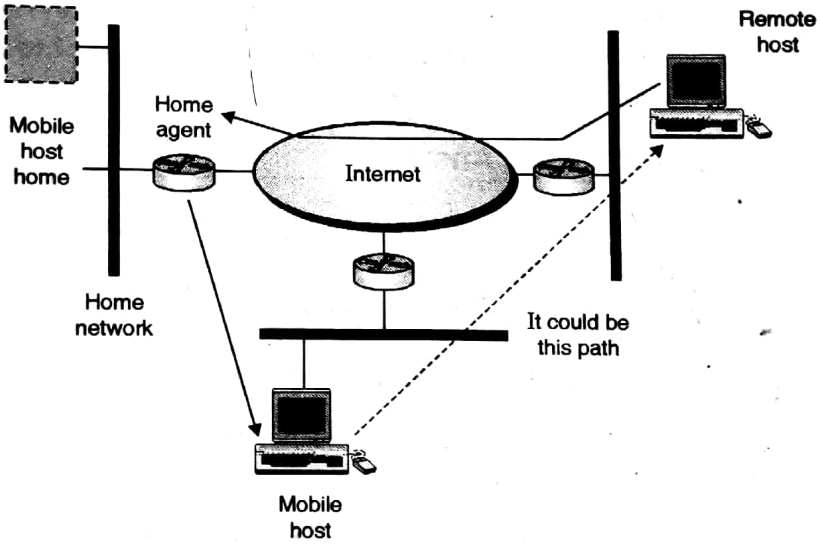


Fig. 2.11.2 : Triangle Routing

Solution for Inefficiency in Mobile IP :

- While doing the communication the remote host should know the mobile host's care-of address so that remote host can send packets through it.
- For example; the home agent tell about mobile host's care-of address to remote host using *update binding packet* while transferring first packet of mobile host so that the remote host can use that care-of address for future communication.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- As mobile host moves its care-of address changes hence home agent needs to send a *warning packet* to the remote host to inform it changes.

Review Questions

Q. 1 Why ARP request is broadcast and Reply is unicast? Explain.
Q. 2 Explain Cache table with reference to ARP.
Q. 3 How output module updates cache table.
Q. 4 RARP request packets are broadcast but reply packets are unicast. Explain.
Q. 5 With the help of a neat diagram explain the fields in RARP packet.
Q. 6 Explain following terms with reference to ARP package.
(a) Cache Table (b) Queues. (c) Output Module.
Q. 7 Write short note on RARP.
Q. 8 How output module updates cache table.
Q. 9 Draw and explain ARP packet format.
Q. 10 Write short note on Mobile IP.
Q. 11 Write short note on ICMP.
Q. 12 Describe ICMP packet format.
Q. 13 Explain various messages in ICMP.
Q. 14 Explain various error reporting messages in ICMP.
Q. 15 Explain various query messages in ICMP.

2.12 University Questions and Answers

April 2013

Q. 1 Explain the Input module of ARP. **(Section 2.7.4)** **(5 Marks)**

Q. 2 What is the inefficiency in mobile IP? Give Solution for it. **(Section 2.11)** **(5 Marks)**

Q. 3 Explain the source quench message and time exceeded message in ICMPv4. **(Section 2.9.1)** **(5 Marks)**

Q. 4 Explain the use of time exceeded message of ICMP. **(Section 2.9.1 (c))** **(5 Marks)**

Q. 5 What are the three phases that a mobile host should go through to communicate with the remote host?

Or

Describe 3 phases of communication between remote host and mobiles host. **(Section 2.10(4))** **(5 Marks)**

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

CHAPTER 3

Routing Protocols

Syllabus

- Unicast Routing Protocols
  - RIP
  - OSPF
  - BGP

3.1 Routing Overview

- Routing is a simple process of selecting paths in a network from multiple available paths along which message can be sent to desired recipient.
- Routing is performed for different networks which includes the electronic data networks like Internet, public telephone networks etc.
- The internet or the electronic networks are works using packet switching technology.
- In such networks, routing will be just a packet forwarding, which transfers logically addressed packets from its source address to their desired destination via intermediate nodes like routers, gateways, bridges etc.

3.2 Routing table

(a) Introduction :

- The routing process usually forwards packets.
- For this function routing tables are used which maintains record of all available routes to various network destinations.

(b) Construction :

- Construction of routing tables is very important function for efficient routing.
- Routing table is generally held in the router's local memory.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(c) Types :

1. Static routing table
2. Dynamic routing table

1. Static Routing table :

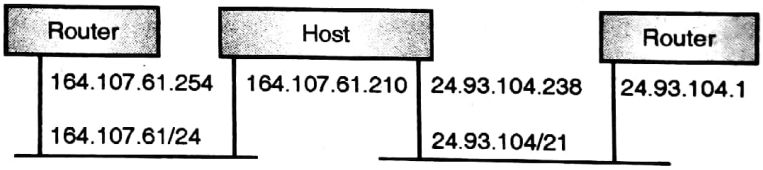
- In this technique routing table is updated with manual data entry.
- Network admin will decide the route from source to destination.
- This type of routing table will not be auto updated as internet properties changes.

2. Dynamic Routing table :

- In this technique routing table is updated on regular basis using dynamic routing protocols.
- Dynamic routing protocols are RIP, BGP and OSPF etc.
- This type of routing table will be auto updated as internet properties changes.

(d) Routing table - Format :

Mask	Network address	Next hop address	Interface	Flag	ReferenceCount	Use
..	..	..	..	..	..	..



Network Address	Network	Gateway address	Interface	Metric
0.0.0.0	0.0.0.0	24.99.104.1	24.99.107.290	1
24.99.104.0	255.255.240.0	24.99.107.290	24.99.107.290	1
24.99.107.230	255.255.255.255	127.0.0.1	127.0.0.1	1
24.255.255.255	255.255.255.255	14.99.107.290	24.99.107.290	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
120.146.0.0	255.255.0.0	164.107.61.254	164.107.61.210	1
164.107.61.0	255.255.255.0	164.107.61.210	164.107.61.210	1
164.107.61.210	255.255.255.255	127.0.0.1	127.0.0.1	1
164.107.255.255	255.255.255.255	164.107.61.210	164.107.61.210	1
224.0.0.0	224.0.0.0	24.99.107.290	24.99.107.290	1
224.0.0.0	224.0.0.0	164.107.61.210	164.107.61.210	1
255.255.255.255	255.255.255.255	164.107.61.210	164.107.61.210	1

Fig. 3.2.1 : Sample routing table

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.3 Autonomous Systems (AS)

1. Introduction :

- An internet is very large hence only one routing protocol cannot handle the task of updating the routing tables of all the routers.
- So an internet is divided in a group of networks and routers which are also known as autonomous systems (AS).

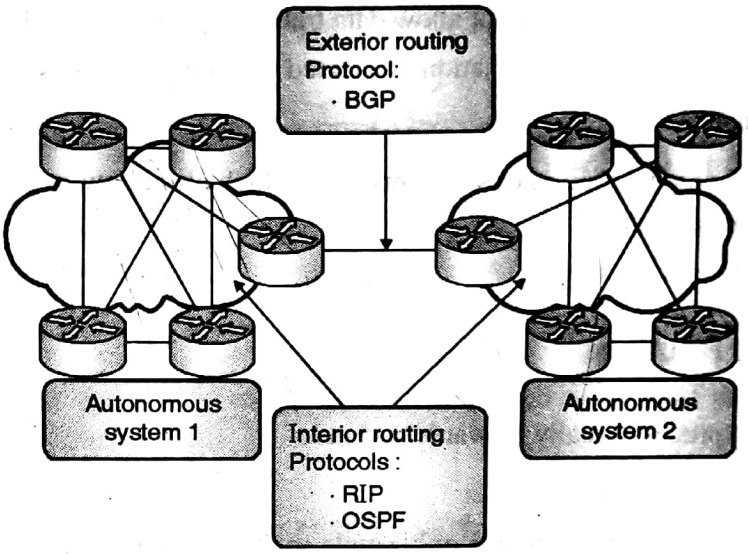


Fig. 3.3.1

2. Types of routing :

(i) **Interior routing :** The routing inside the autonomous systems (AS) is called as interior routing.

(ii) **Exterior routing :** Routing between multiple autonomous systems (AS) is called as exterior routing.

3. Types of autonomous systems (AS) :

(i) **Stub AS :**

- Autonomous systems (AS) which has only one connection with other Autonomous systems (AS) is called as stub AS.
- Any host in AS can send data traffic to other AS.
- Any host in AS can even receive data traffic to other AS.
- Host in stub AS not allow data traffic to pass through it.
- These AS can be either source or sink for data traffic.

E.g. Local ISP

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(ii) Multihomed AS :

- Autonomous systems (AS) which has more then one connection with other Autonomous systems (AS) is also called as Multihomed AS.
- Any host in such type of AS can send data traffic to more then one AS.
- Any host in AS can even receive data traffic from more then one AS.
- Transient traffic not allowed in these contexts.
- These AS can be either source or sink for data traffic.
- Host in such AS not allow data traffic to pass through it.

E.g. Large Organisation connected with more then one regional data traffic.

(iii) Transit AS :

Multihomed Autonomous systems (AS) which also allow transient traffic is called as Transient AS.

E.g. International ISP.

3.4 Types of Routing

The routing process usually forwards packets :

a) Unicast Routing :

In Unicast routing there is only single source and one destination and the relation between the source and destination one is to one.

b) Multicast Routing :

- In multicast routing, there is one source and a group of destinations. So it represents a one is to many relationship.
- So the source address is Unicast address while the destination address is a group of addresses, which defines the members of the group.

3.5 Unicast Routing

1. Introduction :

In Unicast routing there is only single source and one destination and the relation between the source and destination one is to one.

2. Working :

- The source and destination addresses in the IP datagram are unicast addresses assigned to the hosts.
- In this type of routing when a router receives a packet, it forwards that packet through only one of its ports which corresponds to the optimum path.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The router can discard the packet if it can not find the destination address.
- The router accepts the packet only if it find the destination address as own address.
- The unicast routing is illustrated in Fig. 3.5.1.

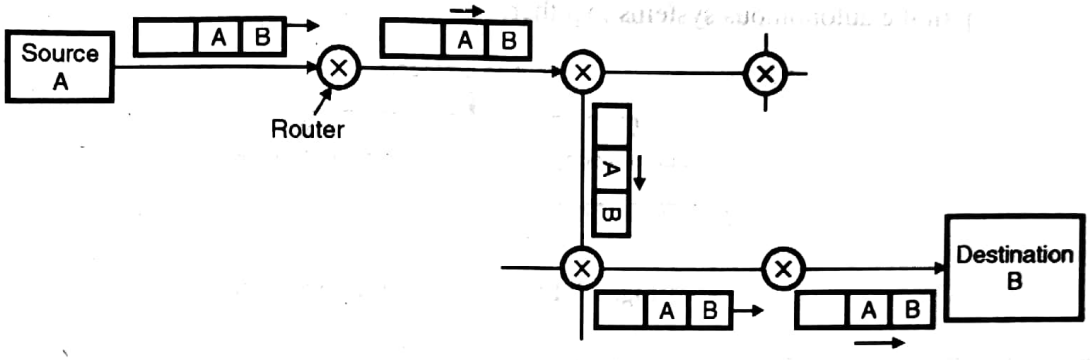


Fig. 3.5.1 : Unicast routing

3. Metric :

- A metric is cost assigned for passing a message through entire a network.
- The metric assigned to each network depends on the type of protocol it is using for routing.

3.6 Unicast Routing Protocols

1. Introduction :

- Routing Protocols are nothing but set of rules and methods which allows routers in internet to inform everyone about change.
- Router can share routing information when it knows about its never in computers and above entire network.

2. Types of routing protocols :

- Interior Routing Protocol
  - Distance Vector Protocol
  - Link State Protocol
- Exterior Routing Protocol
  - Path Vector Protocol

3. Implementation of routing protocols :

- **Routing Information Protocol (RIP)** - It implements Distance Vector Protocol for interior routing.
- **Open Shortage Path First (OSPF)** - It used to implement Link State Protocol for interior routing.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Broader Gateway Protocol (BGP)** - It implements Path Vector Protocol for exterior routing across multiple autonomous systems.
- RIP and OSPF are used to upgrade the routing tables inside an autonomous systems and BGP is used for upgrading the routing tables for the routers which join the autonomous systems together.

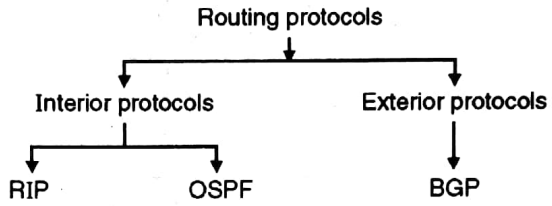


Fig. 3.6.1 : Unicast routing protocols

3.7 RIP (Routing Information Protocol)

1. Introduction :

- It is an interior routing protocol used for interior routing that means routing inside an autonomous system.
- RIP is based on distance vector routing with some Updation.
- RIP uses dynamic, distance vector routing protocol developed for smaller IP based networks.
- RIP uses UDP port 520 for various routing updates.

2. Distance Vector Routing concept :

- In the distance vector routing each router periodically shares its knowledge about the entire network with its neighbours.
- It is one of the simplest routing techniques used for interdomain routing.

3. Routing Table :

- A typical routing table is supposed to keep in every router.
- Destination column consists of the destination network address.
- The other information in Table 3.7.1 may include information such as subnet mask or the time this entry was last updated.

Table 3.7.1 : Routing table

Destination	Hop count	Next router	Other information

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4. Metric :

- RIP calculates the optimal route based on hop count which acts as metric.
- The hop count column consists of the shortest distance to reach the destination and the next router column consists of the address of the next router to which the packet is to be delivered.
- RIP cannot handle more than 15 hops which is called as hop limit.
- Any hop count more than 15 hops away will be considered unreachable.
- This hop limit is useful to prevent routing loops in RIP protocol.

3.7.1 Working of RIP (Using Distance Vector routing) :

1. Initialization of routing table for Update :

1. When a router is added to a network it initialises its routing table.
2. Such a table consists of only the directly attached networks and the hop counts.
3. The next hop field which identifies the next router is empty.

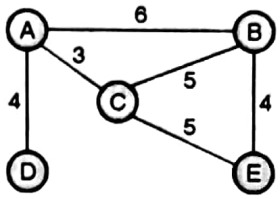


Fig. 3.7.1 : Computer Network

Routing Tables for all nodes above

To	Cost	Next
A	0	--
B	6	--
C	3	--
D	4	--
E	∞	--

Initial Table Node : A

To	Cost	Next
A	6	--
B	0	--
C	5	--
D	∞	--
E	4	--

Initial Table Node : B

To	Cost	Next
A	3	--
B	5	--
C	0	--
D	∞	--
E	5	--

Initial Table Node : C

To	Cost	Next
A	4	--
B	∞	--
C	∞	--
D	0	--
E	∞	--

Initial Table Node : D

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

To	Cost	Next
A	∞	--
B	4	--
C	5	--
D	∞	--
E	0	--

Initial Table Node : E

2. Sharing of routing table for Update :

1. Every neighbouring node knows about it so they need to share information among them.
2. In this technique each neighbours needs to share routing table with immediate nodes wherever there is change in network or also periodically share such information.

3. Updation of routing table for Update :

- When RIP messages are received, each routing table is updated using the RIP updating algorithm.
- **Algorithm for Update**
  - (a) RIP response message is received
  - (b) Add one hop to the hop count for each advertised destination.
  - (c) Repeat the following steps for each advertised destination.
    - (i) Add the advertised information to the table if the destination is not present in routing table.
    - (ii) Replace entry in the table with the advertised one if the next hop field is same.
    - (iii) Replace entry in the routing table if advertising hop count is smaller than one in the table.
    - (iii) Return

To	Cost
A	3
B	5
C	0
D	∞
E	5

Table form Node C

To	Cost	Next
A	6	C
B	8	C
C	3	--
D	∞	--
E	8	C

Compare

Modified Table Node A

To	Cost	Next
A	0	--
B	6	--
C	3	--
D	4	--
E	∞	--

Initial Table Node A

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

To	Cost	Next
A	0	--
B	6	--
C	3	--
D	4	--
E	8	C

New routing Table Node : A

4. Final of routing table after Update :

- When RIP messages are received, each routing table after update, given as below,
- Final Routing Tables for all nodes,

To	Cost	Next
A	0	--
B	6	--
C	3	--
D	4	--
E	8	C

Final Table Node : A

To	Cost	Next
A	6	--
B	0	--
C	5	--
D	10	A
E	4	--

Final Table Node : B

To	Cost	Next
A	3	--
B	5	--
C	0	--
D	7	A
E	5	--

Final Table Node : C

To	Cost	Next
A	4	--
B	10	A
C	7	A
D	0	--
E	12	A

Final Table Node : D

To	Cost	Next
A	8	C
B	4	--
C	5	--
D	12	C
E	0	--

Final Table Node : E

3.7.2 Two-Node Loop Instability :

Q. Explain the two-node loop problem of distance vector routing. Give the solution of it.

MU - April 2013

Major problem with distance vector routing is instability, which means that a network using distance vector routing protocol can become unstable.

The following Fig.3.7.2 shows a system having three nodes X, A and B.

1. Firstly there is path to reach node X from Node A and B;

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

From Node A it has distance 2 and From Node B it takes 6 { i.e 4 (to reach A) + 2 (from A) } but suddenly the link between node X and A fails.

2. Node A updates its routing table. If node A not able to send updated table to node B system becomes unstable.B sends its routing table to node A before getting A's updated routing table.
3. Node A assumes that Node B got the link to reach Node x and immediatly updates own routing table.
4. As triggered update routing table strategy Node A sends its updated table to Node B.

   Node B thinks that some changes are happend with the links from Node A and again updates its table which having link from A.
5. Cost of reaching X from node A and B increases gradually till it reaches infinity. During this update sharing the system becomes unstable.
6. Node A and Node B both thinks that they have path to reach Node X and they keep on transffering packets to each other which are related to Node X. Since there is no path to reach X the packet comes back to the source node and the packet keeps on bouncing between Node A and B. It creates a Two-node loop Problem.

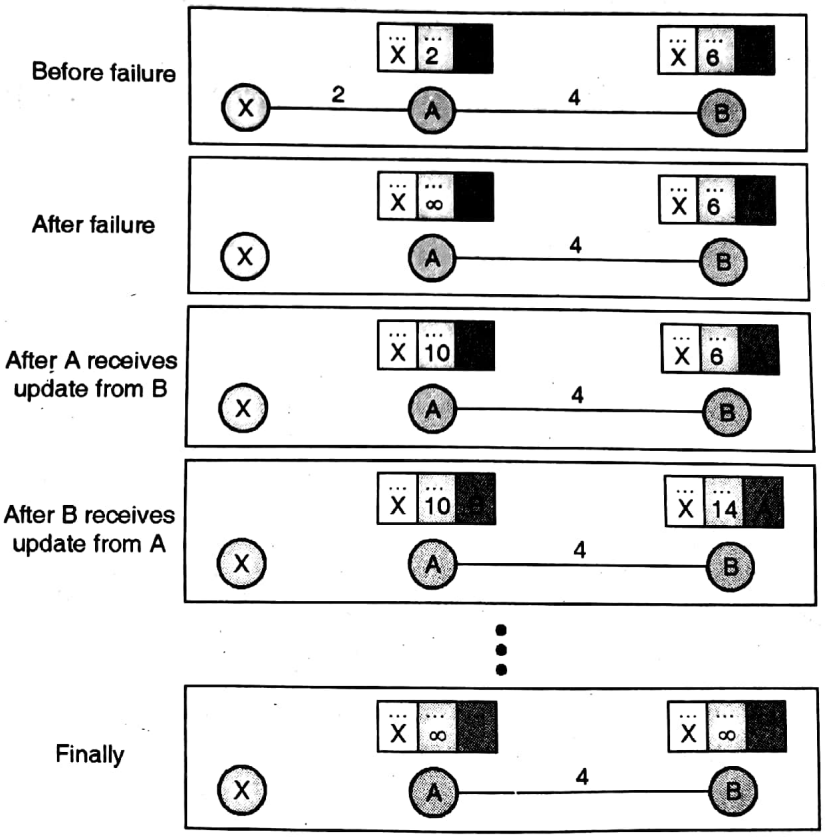


Fig. 3.7.2 : Two-Node Loop Instability

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Solutions to two-node loop instability are as follows:

Defining Infinity :

- To avoid this loop problem in the system; solution is to re-assign the infinity to a smaller updating range. It means we will keep a smaller value for update sharing.
- Most distance vector protocol related implementation uses update range minimum 1 and maximum 16 as infinity.
- Due to this distance vector routing can not be useful in large systems.

Split Horizon :

- In the split horizon method; each node just sends part of updated table in the interface to each other to avoid unnecessary flooding of information. No need of advertising the known information again to same node.
- Taking updated table information from node A; Node B again updates it as per current scenario and sends it back to node A creates misunderstanding.
- While sending routing table to node A; Node B does not passes last line of routing table.
- Instead of infinity value Node A keeps it as distance between A to X .After the updating it transfers table to Node B than node B also updates it as per node A's updating ; finally it clears that there is no path to reach Node X from Node A as well as from node B.

Split Horizon and Poison Reverse :

- In this strategy combination of split horizon and poison reverse is used.
- Distance vector routing uses timer; If Node B does not get information about route to reach X it simply eliminates route to reach X from its advertisement to node A.
- Node B can still advertise the value of node X if the source is other than Node A, but if the source of information is A, it can replace the distance with infinity as a warning which specify "Don't use this value; what I know about this route comes from you."

3.7.3 RIP Operation :

1. RIP forms routing database which stores information about the fastest route from computer to computer, this update process that enables each router to tell about other routers which may route faster from neighboring routers.
2. Each router on the internet has a database that stores the following information,

   IP Address

   It is a Logical address of the computer.

   Gateway

   The best gateway to send a message addressed to required IP address.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Distance

It is number of routers between source router and the destination router.

Route change flag

This flag indicates that this information has updated by other routers to update their own databases.

Timers

Various timers are used with RIP.

3. Each router periodically sends an update message about its routing database to all the other routers that it is directly connected. Some routers will send this message after every 30 seconds, so that the network will always have up-to-date information to about them. It can quickly adapt to changes as computers and routers come on and off the network.
4. RIP will make use of the UDP network protocol because it is efficient, and there are no problems if a message gets lost due to any reason, which is fine for router updates where another update will be coming along shortly anyway.

3.7.4 RIP Message Format :

- RIP messages are of two types :
  - Routing information messages
  - Routing information request message
- Both use the same format which consists of a fixed header followed by an optional list of network and distance pairs.

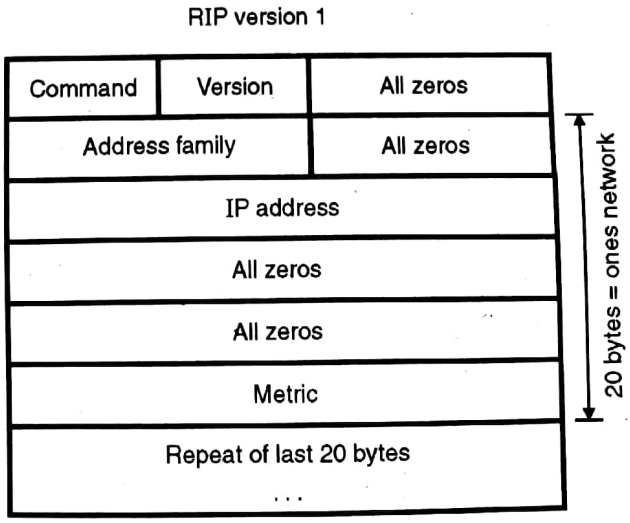


Fig. 3.7.3 : RIP Message Format

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(a) Command :

- This field shows the packet is either request or a response packet.
- The request asks that a router send all or part of its routing table as a message.
- The response can be a reply to a request or an unsolicited regular routing update.
- Responses may contain some or all routing table entries.

(b) Version number :

Specifies the RIP version used.

(c) Address-family identifier (AFI) :

- This field shows the address family used.
- RIP is designed to carry routing information for several different protocols.
- The AFI for IP is 2.

(d) Address :

- This field shows the IP address for the entry.

(e) Metric :

- This field shows how many inter network hops (routers) have been crossed in the trip to the destination.
- This value is between 1 and 15 is for a useable route, or 16 used for an unreachable route.

3.7.5 RIP Timers :

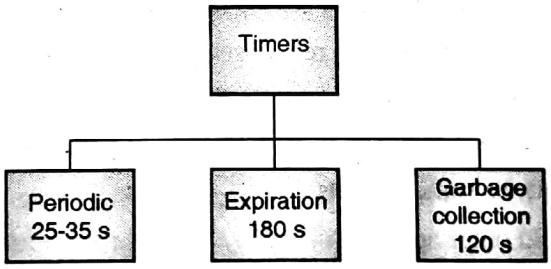


Fig. 3.7.4

1. Periodic Timer :

- It is mainly used for sending periodic update messages.
- As per protocol time should be 30 Seconds but generally we use any random number between 25 to 35 seconds periodic timer.
- It avoids overhead on internet from simultaneous update of routers.
- When it reaches zero update messages sent and timer set again to original value.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.I.T Study

2. Expiration Timer :

- It used to check validity of route.
- Every route have own expiration timer.
- When router receives update message for route expiration timer set to 180 seconds.
- Whenever router receives new update message expiration timer resets after 30 seconds.
- If no update from last 180 seconds route considers as expire and hop count will be set to 16 that means destination is unreachable.

3. Garbage Collection Timer :

- Invalid path are immediately not removed from table. But advertise about it with value 16.
- For such route garbage collection timer set to 120 seconds, when it reaches zero route will be removed from table.
- With help of this timer neighbour will come to know about invalid paths.

3.7.6 Disadvantages :

1. RIP only knows the shortest route to a destination, established on simple count of router hops.
2. It be determined by other routers for computed routing updates.
3. Routing tables are broadcasted every 30 seconds.
4. Distances are based on hops, not on real costs.
5. Patched with split horizon poison reverse, hold down timers, triggers updates.
6. It continues to be a router to router configurations, one router is fully depend on the next router to implement the same options.
7. Fix one problem and other appears.

3.8 OSPF (Open Shortest Path First)

Q. Explain the following terminologies related to OSPF protocol MU - April 2013

(i) Area (ii) Metric (iii) Link state database

1. Introduction :

- This is yet another good interior routing protocol.
- OSPF will handle the routing efficiently and in more timely manner.
- The OSPF will divide an Autonomous System into multiple areas.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- This protocol implements link state routing protocol.

2. Metric :

- The cost assigned to each router is called as metric.
- In the OSPF protocol the metric can be based on a type of service provided.
- A router can have multiple routing tables based on different types of service.

3. Area :

- A collection of networks computers and routers is called as an area.
- Single autonomous system can be divided in various areas.

Area Border routers

These are special type of routers which are used at the borders of an area.

4. Backbone :

- A special area inside an autonomous system is called as backbone.
- All the areas inside an A.S. should be connected to the backbone.
- This backbone is acts like a primary area and other areas are secondary areas.
- **Backbone routers**
  - The routers within the backbone are called as the backbone routers.
  - Such backbone router can also be an area border router.

5. Area identification :

- Each area has area identification.
- The area identification of the backbone is zero.

3.8.1 How OSPF Solve Problems Faced by RIP ?

- The first shortest-path-first routing protocol was developed and used in the ARPAnet packet switching network all the way back in 1978.
- This first shortest path first routing protocol is used in OSPF.
- OSPF provides solutions to the major problems in RIP.
- Routing architectures can balance well after the maximum of 16 hops are supported by RIP.
- OSPF routers interchange link state information in place of exchanging node reachability information.
- *Link state routing overview*

  In case of Link state information, every router maintains its personal copy of the network topology. Used for, shortest path routing decisions can then be taken.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.8.2 Features :

1. **Type of Service routing :**
   - Various routes are arranged to support multiple type of service requirements.
   - Example, high-throughput can be selected for one class of service, while minimal delivery delay is critical for some other type of application.
2. **Load Balancing :**

   When many routes are available, traffic can be evenly distributed over these different routes.
3. **Subdivision of Autonomous Systems :**

   Dividing the system into logical areas can enhance management of large autonomous systems.
4. **Security :**
   - The exchange of Data is authenticated hence automatically secure.
   - Malicious transmissions from foreign routing nodes are avoided.
   - Only those hosts intended for the routing network are included.
5. **Host :**

   Specific network and sub network routing are supported.
6. **Special features are provided to support LAN environments :**
   - Relationships between routers are maintained on a logical link.
   - Link state transmissions are minimized.
   - **Designated gateways** are responsible for transmitting the link state information in their local area.
7. **OSPF is an open specification :**
   - Published as an RFC rather than specified standard.
   - The intent is to encourage many vendors to use it rather than requiring users to lock into a single vendor's equipment.
8. **OSPF area :**
   - OSPF allows the grouping of networks into a logical set which is also called as called an **area**.
   - The topology of an area is hidden from the other Autonomous System.
   - This technique minimizes the routing traffic required for the protocol.
   - When multiple areas are used, each area has its own copy of the topological database.
   - Multiple concepts are involved with the OSPF algorithm.
   - RIP is gives autonomous system by way of a monolithic group of routes and subnets, OSPF introduces the concept of **area**, which can be used for hiding

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

routing information within a OSPF routing domain.

- Autonomous system is separated into a various logical areas; various OSPF routing nodes are supported, with internal routers, area border routers, backbone routers, and Autonomous System (AS) boundary routers.
- The protocols used to support link state change broadcasts.
- A "Hello" protocol is used to detect changes in the availability of neighboring routers.

3.8.3 Types of Links :

- In the OSPF any connection is called as a link.
- It defines four types of links called point to point, transient link, stub link and virtual links

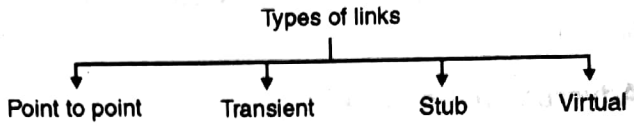


Fig. 3.8.1 : Types of links

1. Point to point link :

- This link joins two routers without any other host or router in between them.
- E.g. Two routers connected by a telephone line.
- Each router has only one neighbor at the other side of the link.
- This is shown in Fig. 3.8.2.

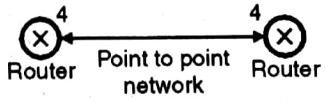


Fig. 3.8.2 : Point to point link

2. Transient link :

- It is a network having many routers attached to it.
- All LANs are of this type.
- A, B, C ….. etc. are the routers.
- Each router has several neighbors.

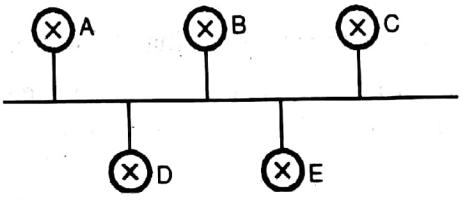


Fig. 3.8.3 : Transient link

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3. A stub link :

- A stub link is a network that is connected to only one.

(a) Stub network **(b) Representation**

Fig. 3.8.4

- The stub network of is a special case of transient network.
- The data packets enter the network through this single router and leave the network through the same router.
- Virtual link: A virtual link is created between two routers when the link between them is broken.

3.8.4 Link State Advertisements (LSA) :

- Each entity in a network distributes the link state advertisements (LSAs).
- An LSA announces the states of entity links.
- Different types of LSA depending on the type of entity.

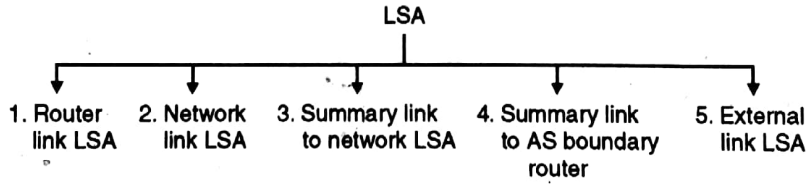


Fig. 3.8.5 : Types of LSA

(a) Router Links :

- The router invents a router links advertisement on behalf of each area to which it belongs.
- The advertisement refers to the collected states of the router's links to the area.
- This advertisement furthermore indicates if the router is an area border router or an AS boundary router.

(b) Network Links :

- A network link advertisement is originated for every transit multi-access network.
- This advertisement is originated by the designated router for the transit network, and describes all the OSPF routers fully adjacent to the designated router.

(c) Summary Links :

- Summary Link advertisements designate a single route toward a destination.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The destinations designated to the area but internal to the Autonomous System.
- Some routing information is reduced while creating these summary link state advertisements.

(d) AS Summary Links :

These are siinilar to summary link advertisements but they routes to Autonomous System boundary routers.

(e) AS External Links :

AS external advertisements define routes external to Autonomous System.

3.8.5 OSPF Working :

- The OSPF protocol runs directly over IP by assigned number 89.
- Each OSPF packet consists of an OSPF header followed by the body of a particular packet type.
- OSPF packets need to be sent to specific IP addresses in non broadcast multi-access networks.
- The OSPF operation consist of following stages :
  - Neighbors are discovered trough the sending of Hello messages and designated routers are elected in multi-access networks.
  - Adjacencies are established and link state databases are synchronized.
- Link state advertisements (LSA) are exchanged via adjacent routers for topological databases to be maintained and to advertise inter area and inter AS routes.
- The routers usage the data in the database to generate routing tables.

3.8.6 Link State routing using Dijstra's Algorithm :

1. Initialization of routing table for Update :

When a router is added to a network initialises its routing table with empty tables.

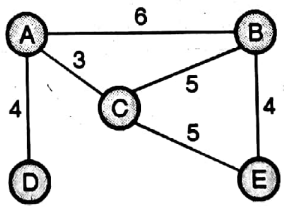


Fig. 3.8.6

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Routing Tables for all nodes above

To	Cost	Next

Initial Table Node : A

To	Cost	Next

Initial Table Node : B

To	Cost	Next

Initial Table Node : C

To	Cost	Next

Initial Table Node : D

To	Cost	Next

Initial Table Node : E

2. Finding shortest path using Dijstra's algorithm :

Each node will search for shortest path from that node to each source node using below given Dijstra's Algorithm.

Algorithm for Update

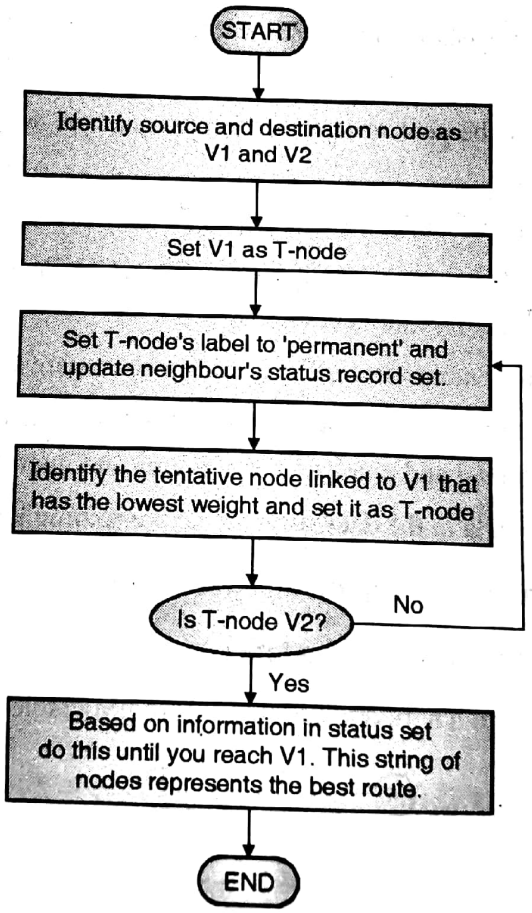


Fig. 3.8.7 : Dijstra's algorithm

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

To	Cost	Next
A	0	--
B	6	--
C	3	--
D	4	--
E	8	C

New routing Table Node : A

3. Final of routing table after Update :

- Apply same method for all routing tables and find shortest distance from node to node.
- Final Routing Tables for all nodes

To	Cost	Next
A	8	C
B	4	--
C	5	--
D	12	C
E	0	--

Final Table Node : E

To	Cost	Next
A	6	--
B	0	--
C	5	--
D	10	A
E	4	--

Final Table Node : B

To	Cost	Next
A	3	--
B	5	--
C	0	--
D	7	A
E	5	--

Final Table Node : C

To	Cost	Next
A	4	--
B	10	A
C	7	A
D	0	--
E	12	A

Final Table Node : D

3.8.7 OSPF Packet Format :

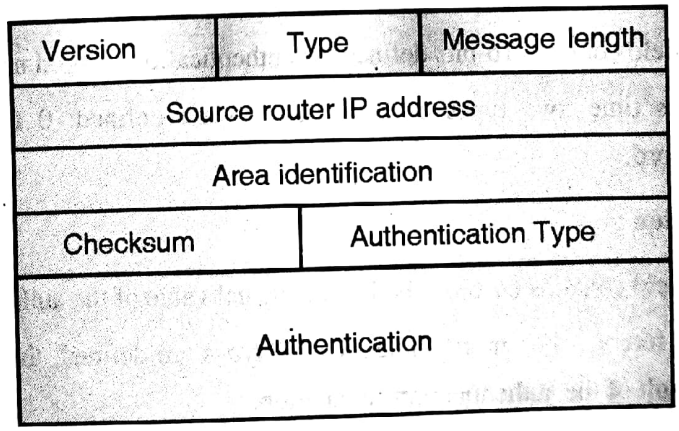


Fig. 3.8.8 : OSPF packet header

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(a) Version :

- This field contains 8-bit field which defines the version of the OSPF protocol.
- It is currently version 2.

(b) Type :

- This field contains 8-bit which defines the type of the packet.
- There are five types, with values 1 to 5 defining the types.

(c) Message length :

This field contains 16-bits which defines the length of the total message including the header.

(d) Source router IP address :

This field contains 32-bits defines the IP address of the router that sends the packet.

(e) Area identification :

This field contains 32-bits defines the area within which the routing takes place.

(f) Checksum :

This field is used for error detection on the entire packet excluding the authentication type and authentication data field.

(g) Authentication type :

- This field contains 16-bits defines the authentication method used in this area.
- At this time, two types of authentication are defined: 0 for none and 1 for password.

(h) Authentication :

- This field contains 64-bits which is the actual value of the authentication data.
- In the future, when more authentication types are defined, this field will contain the result of the authentication calculation.
- For now, if the authentication type is 0, this field is filled with 0s.
- If the type is 1, this field carries an eight-character password.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.8.8 OSPF Packet Types :

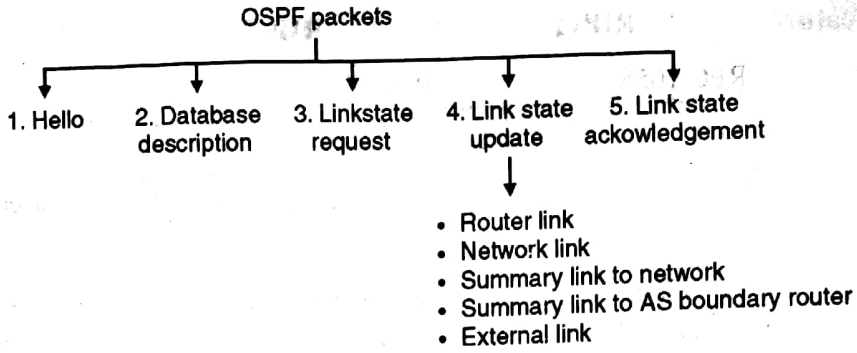


Fig. 3.8.9 : OSPF packet types

The protocol utilizes five different packet types.

1. **Hello :**

   Used to discover and maintain information about neighbors.

2. **Database Description :**

   - It is used to form adjacencies between multiple nodes.
   - The router summarizes all its link state advertisements and passes information, using database description packets to the all other routers.

3. **Link State Request :**

   - After the database description packets have been exchanged with neighbouring routers, to detect link state advertisements to update the topological database.
   - Link state request packets are sent to the neighbor requesting these link state advertisements.

4. **Link State Update :**

   - Used for transmission of link state advertisements between various routers.
   - This can be in response to any link state request packet or to flood a new or more recent link state advertisement.

5. **Link State Acknowledgment :**

   - Used for the flooding of link state advertisements reliable.
   - Each link state advertisement received should be acknowledged.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.8.9 Comparison between RIP and OSPF :

Function/Feature	RIPv1	RIPv2	OSPF
Standard number	RFC 1058	RFC 1723	RFC 2178
Link-state protocol	No	No	Yes
Large range of metrics	Hop count (16=Infinity)	Hop count (16=Infinity)	Yes, based on 1-65535
Update policy	Route table every 30 seconds	Route table every 30 seconds	Link-state changes, or every 30 [minutes]
Update address	Broadcast	Broadcast, multicast	Multicast
Dead interval	300 seconds total	300 seconds total	300 seconds total, but usually much less
Supports authentication	No	Yes	Yes
Convergence time	Variable (based on number of routers X dead interval)	Variable (based on number of routers X dead interval)	Media delay + dead interval
Variable-length subnets	No	Yes	Yes
Supports supernetting	No	Yes	Yes
Type of Service (TOS)	No	No	Yes
Multipath routing	No	No	Yes
Network diameter	15 hops	15 hops	65535 possible
Easy to use	Yes	Yes	No

3.9 BGP (Border Gateway Protocol)

Introduction :

- BGP is an exterior routing protocol which can transfer data across various autonomous systems.
- It is a unicast routing protocol introduced in 1989 and has four different versions.
- BGP is based on the routing method called **path vector routing**.
- This principle is used because the distance vector routing and link state routing do not prove to be good candidates for inter autonomous system routing.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.9.1 Path Vector Routing :

Q. Explain path vector routing. MU - April 2013

1. Introduction :

In this technique each entry in the routing table contains the destination network, the next router and the path to reach the destination.

Table 3.9.1 : Path vector routing table

Network	Next router	Path
N01	R01	AS 12, AS 21, AS 56
N02	R08	AS 20, AS 57, AS 06
.	.	.
.	.	.
.	.	.

2. Path Vector Message :

- The boundary routers which participate in path vector routing, advertise the Reachability of various network from it.
- Every router that receives a path vector message will verifies that the advertised path is according to its policy.
- If yes then the router will update its routing table and then modifies the message before sending to the next neighbouring node.
- In the modified message it sends its own AS number and replaces the next router entry with its own identification.

3. Path Prevention :

- The autonomous boundary routers which participate in path vector routing,
- When a message is received, a router checks it to see if its autonomous system is in the path list to the destination. If it is then looping is necessary and the message is ignored.

4. Path Attributes :

The path is specified in terms of attributes. Each attribute gives some information about the path. Hence the list of attributes helps the receiving router to make a better decision about when to apply its policy.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Attributes are of two types :

a) **Well known attribute**

A well known attribute is the one which should be recognised by every BGP router.

b) **Optional attribute**

An optional attribute is the one that need not be recognised by every router.

3.9.2 Types of Messages :

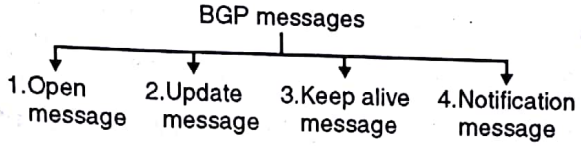


Fig. 3.9.1 : BGP message types

1. **Keep Alive Message :**

- This message opens a BGP session between various nodes and is the first message sent by each side after a connection is established.
- Open messages are confirmed using a keep-alive message sent by the peer device.
- Such message must be confirmed before updates, notifications, and keep-alives can be exchanged.
- The keep-alive message notifies BGP that a device is active.
- Keep alive message are sent often enough to keep the sessions alive.

2. **Update Message :**

- An update message is used to provide routing updates to other BGP systems.
- Routers to construct a consistent view of the network topology using above updates.
- Updates are generally sent using the TCP.
- Update messages can withdraw one or more unfeasible routes from the routing table then advertise a route while withdrawing others.

3. **Notification Message :**

- The notification messages are sent when some error condition detected by network.
- Notifications are used to close an active session and to inform any connected routers.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3.9.3 BGP Header Format :

(a) Introduction :

- The BGP header contains Open, update, and notification messages have additional fields and keep-alive messages use only the basic packet header.
- Each BGP packet will contains a header whose main purpose is to identify the function of the packet in question.

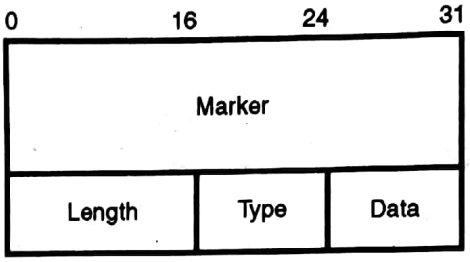


Fig. 3.9.2 : BGP packet header

(b) Header Fields :

Marker

Contains an authentication value that the message receiver can predict.

Length

Indicates the total length of the message in bytes. The value of the length field must be between 19 and 4096.

Type

Type specifies the message type as one of the following :

(a) Open (b) Update

(c) Notification (d) Keep-alive

Data

Contains the upper layer information in this optional field.

3.9.4 BGP Operation :

1. Routing involves two basic activities
   (a) Determination of optimal routing paths
   (b) Transport of packets through an inter network
2. The transport of packets through an network is relatively simple process. In which path determination, can be a very complex.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Protocol which addresses the task of path determination is the Border Gateway Protocol (BGP). BGP performs interdomain routing in TCP/IP networks.

3. BGP is an exterior gateway protocol (EGP), It performs routing between multiple autonomous systems and exchanges routing and Reachability information with other BGP systems.
4. BGP was developed to replace Exterior Gateway Protocol (EGP), as the standard exterior gateway-routing protocol. BGP solves serious problems with EGP.
5. EGP is a instance of an exterior gateway protocol.

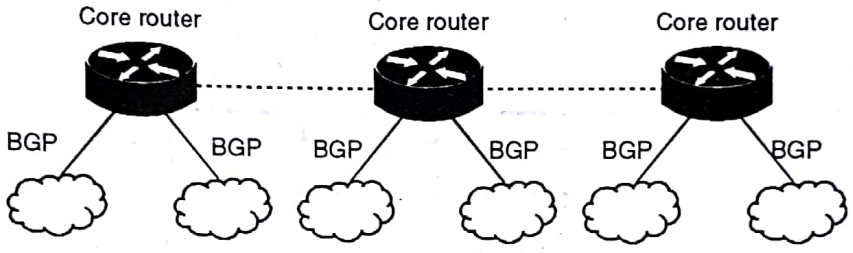


Fig. 3.9.3 : Core routers can use BGP to route traffic between autonomous systems

3.9.5 IGP and EGP :

1. A router in a transit Autonomous System (AS) can have large routing tables and BGP-4 makes use of Classless Inter Domain Routing (CIDR) to slow the growth of these tables.
2. The router maintains routing tables can exchange IGP and BGP information between them.
3. There are two types of sessions (among router and its neighbors) :
   - **(a)** **Exterior Gateway Protocol (EGP)** sessions occur between routers in different Autonomous System (AS), which are usually neighbors to each other sharing the same media and subnet.
   - **(b)** **Interior Gateway protocol (IGP)** sessions occur between routers within the same Autonomous System (AS) and these sessions are used to synchronize the routing policy within same Autonomous System (AS).

     Such routers do not have to be next to each other however they do need to be able to see each other a TCP connection.
4. Interior Gateway protocols use metric interface costs (OSPF) or hop counts (RIP) to determine the best paths.
5. Exterior Gateway Protocols are used to administer routing policies to determine best paths through service providers.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

6. EGP used by old Internet topology, due to its small size, was a simple two-tier model.
7. Autonomous System (AS) was given a 16-bit number and every 3 minutes EGP advertised the routes that it knew with other EGP.
8. **Problem with EGP**

   It could not cope with a meshed network of AS.

   EGP could not detect loops and no way for creating policies for routing.

3.9.6 Types of Routing in BGP :

BGP performs three types of routing :

(a) Inter autonomous system routing :

- Inter autonomous system routing occurs between two or more BGP routers in different autonomous systems.
- Peer routers in these systems use BGP to maintain a consistent view of the inter network topology.
- BGP neighbouring routers communicating between autonomous systems must be in the same physical network.
- Many of these domains represent the various corporations, institutions and entities which make up the Internet.
- BGP is frequently used to for path determination for offering optimal routing within the Internet.

(b) Intra-autonomous system routing :

- Intra autonomous system routing happens between two or more BGP routers located in the same autonomous system.
- BGP is used to maintain a consistent view of the system topology in peer routers within the same autonomous system use.
- BGP also is used to determine which router will serve as the connection point for specific external autonomous systems.
- An organization, such as a university, could make use of BGP to provide optimal routing within its own administrative domain or autonomous system.
- The BGP protocol can provide both inter as well as intra autonomous system routing services.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(c) Pass-through autonomous system routing :

- Pass-through autonomous system routing occurs between two or more BGP peer routers which exchange traffic across an autonomous system that does not run using BGP.
- The BGP traffic did not originate or terminated on the autonomous in a pass through autonomous system environment.
- Fig. 3.9.4 illustrates a pass-through autonomous system environment: BGP pairs with another intra-autonomous system-routing protocol.

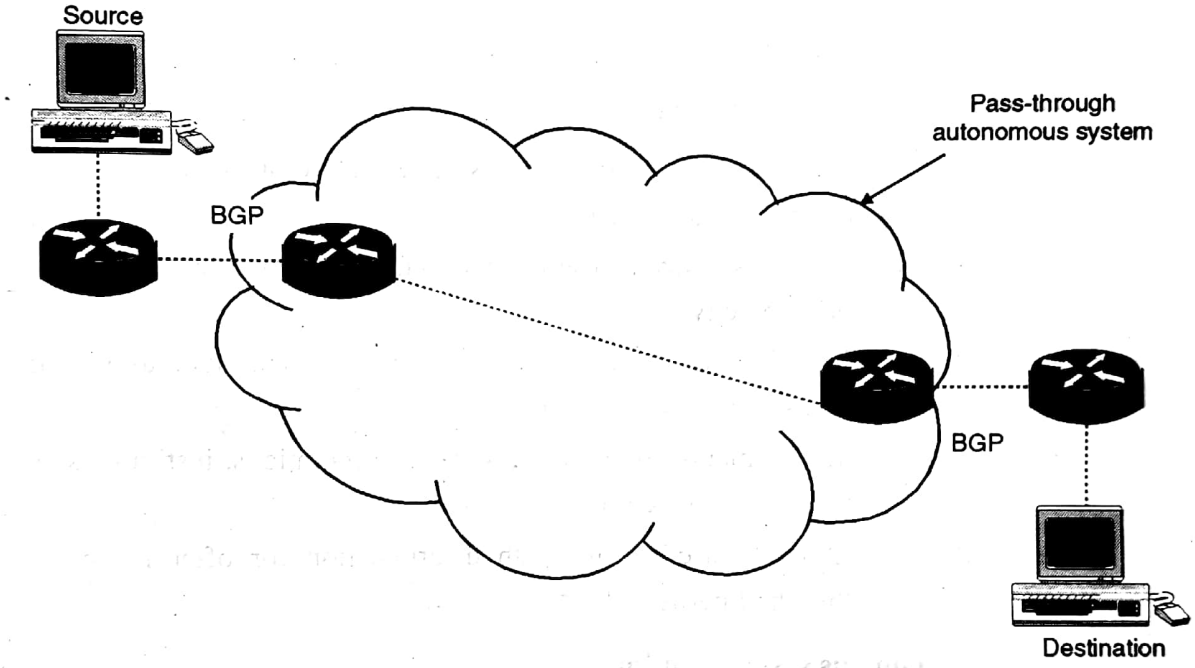


Fig. 3.9.4

3.9.7 BGP Working for Routing :

1. BGP maintains routing tables and transfers routing updates and makes routing decisions on routing metrics.
2. BGP system exchanges network reachability information, including information about the list of autonomous system paths, with other BGP systems.
3. Such information can be used to construct a graph shows connectivity of autonomous systems from which routing loops can be reduced.
4. BGP router records a routing table which lists all feasible paths to a particular network.
5. The router does not refresh the routing table.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

6. Routing information received from other routers is preserved until an incremental update is received.
7. BGP devices exchange routing information for initial data exchange and also after incremental updates.
8. After initial connection with network, BGP routers exchange their all BGP routing tables. When this tables changes, routers send the portion of their routing table which is actually changed.
10. BGP routers do not send regular routing updates.
11. BGP routing updates advertise only the optimal path to a network.
12. BGP uses only one routing metric to determine the optimal path to a given network which consists of an arbitrary unit number that specifies the degree of preference of a particular link.
13. The BGP metric assigns network administrator to each link.
14. The value assigned to a link can be based on any number of criteria, including the number of autonomous systems through which the path passes stability, speed, delay or cost.

Review Questions

Q. 1 What do you mean by routing? Explain various types of routing techniques.

Q. 2 Explain Autonomous system and its various types used in BGP.

Q. 3 Explain routing table in details with example.

Q. 4 Explain various routing techniques and its algorithms.

Q. 5 What do you mean by routing? Explain various inter domain routing techniques.

Q. 6 Describe distance vector routing techniques with example.

Q. 7 Write a short note on RIP.

Q. 8 Write a short note on RIP header format.

Q. 9 Explain RIP request and response packets.

Q. 10 Write a short note on RIP timers.

Q. 11 Describe Link state routing techniques with example.

Q. 12 Write a short note on OSPF protocol.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Q. 13 Explain various types of links in OSPF.

Q. 14 Describe OSPF header packet.

Q. 15 Describe path vector routing techniques with example.

Q. 16 Write a short note on BGP.

Q. 17 Describe header packet format of BGP.

Q. 18 Explain various types of message in BGP.

Q. 19 Discuss various Unicast routing protocols in details.

Q. 20 Compare various Unicast routing protocols.

3.10 University Questions and Answers

April 2013

Q. 1 Explain the following terminologies related to OSPF protocol **(Section 3.8)** **(5 Marks)**

(i) Area (ii) Metric (iii) Link state database

Q. 2 Explain path vector routing. **(Section 3.9.1)** **(5 Marks)**

Q 3 Explain the two-node loop problem of distance vector routing. Give the solution of it. **(Section 3.7.2)** **(5 Marks)**

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

CHAPTER 4

Transport Layer Protocols

Syllabus

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)

4.1 Transport Layer

Introduction :

- The OSI Layers which are helps to transfer packet from one end to other are:
  - Network layer
  - Data link layer
  - Physical layer
- To pass message from one process to another process is done with the help of transport layer in the network.
- In transport layer to handle the transmission of messages in the network without any issues some protocols are used.
- The transport layer protocols are listed below :
  - **UDP (User Datagram Protocol) :**
    It provides a programming interface and not able to implement any real function
  - **TCP (Transmission Control Protocol) :**
    It helps to implement error recovery, flow control etc.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

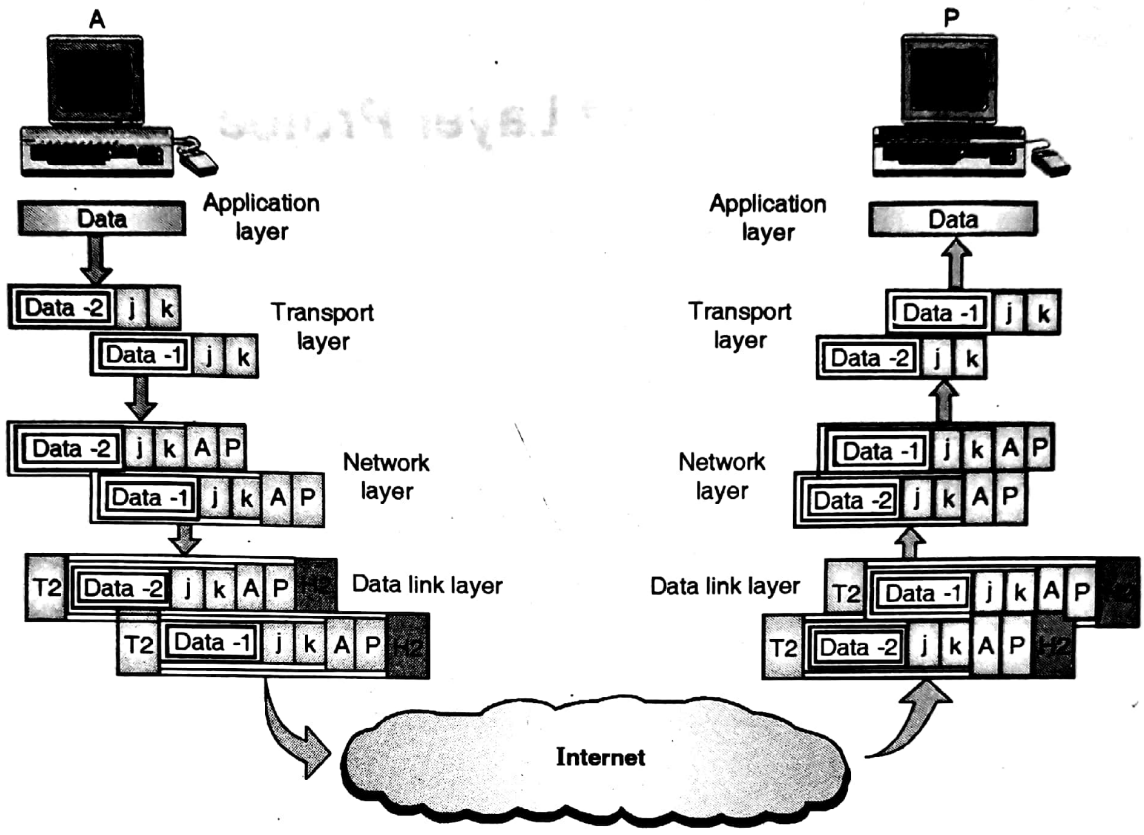


Fig. 4.1.1 : User Datagram Protocol

4.2 UDP

4.2.1 The Position in OSI Model :

- UDP is transport layer protocol.
- UDP helps to transfer the message from one process to another process in the network.
- It is known as *connection less* protocol it means there is no need of prior connection between client and server to do data transmission.
- Whenever data is forwarded from client for particular destination then the UDP packet is forwarded via the number of OSI layer without any established connection.
- The UDP able to send message with the maximum size as 8 Kbytes.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

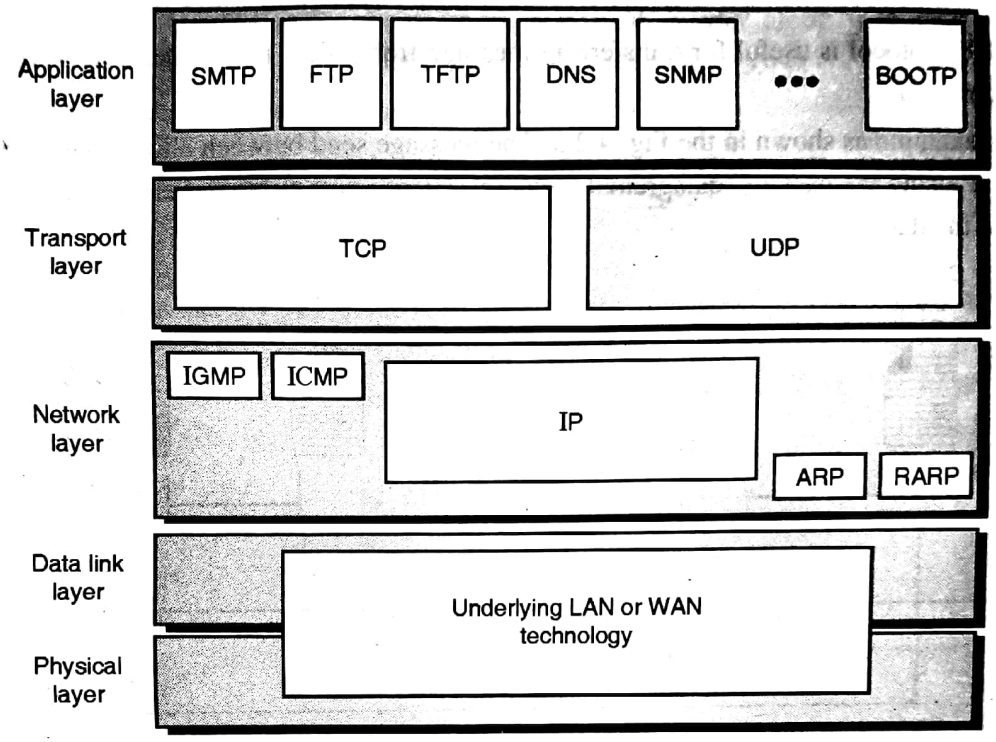


Fig. 4.2.1

4.2.2 UDP vS IP :

- The IP protocol from network layer helps to transfer message form particular system to system.
- The UDP protocol from transport layer helps to transfer messages from process to process as shown in the Fig. 4.2.2.

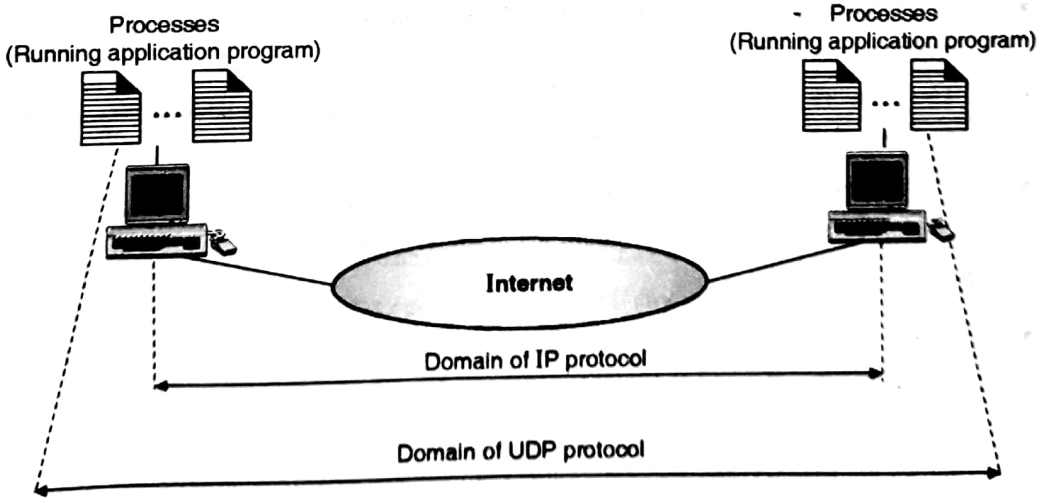


Fig. 4.2.2

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.2.3 Port Number :

- UDP protocol is useful for transferring message from client port to destination port and vice versa.
- As example as shown in the Fig. 4.2.3. The message send between client UDP to Server UDP using the packets (datagrams) including client's port number, Server's port number and the data.

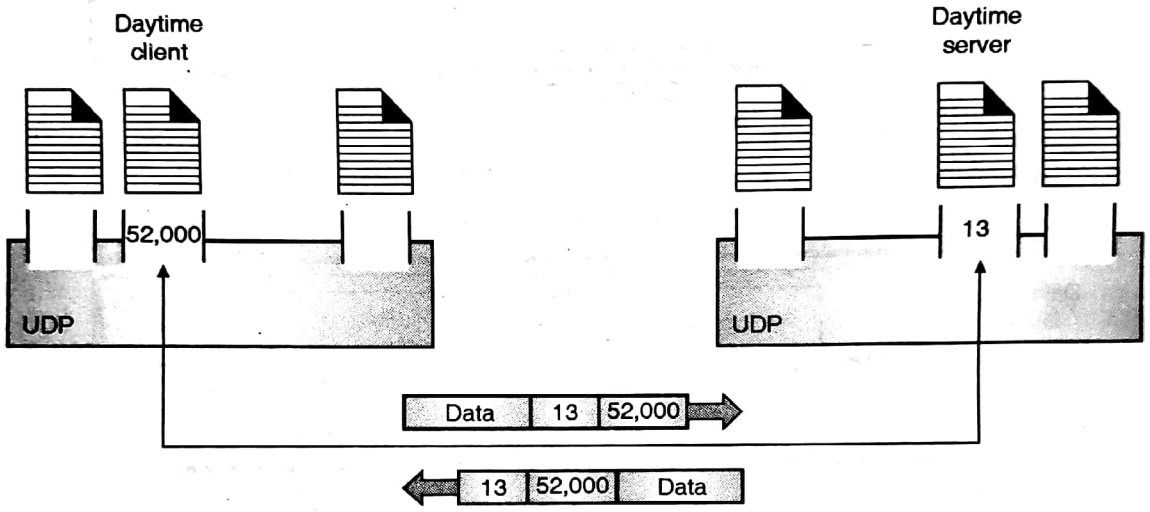


Fig. 4.2.3

4.2.4 How Data Transfer Takes Place ?

(a) Client side :

- When message is transferred from client to server it forwarded via layers like transport layer, network layer, data link layer and physical layer.
- The transport layer forward packet (UDP Datagram + UDP header) to the next layer i.e. network layer.
- The network layer consider whole as IP data and adds own header i.e. IP header than forwarded it to the lower layers.
- The lower layers consider the message as frame data and then add its frame header. Finally the message becomes ready to transmit over the network.

(b) Server side :

- When the message reaches to the destination it first passes through the lower layers where the added header from client side layers detached and then forwarded to next layer.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Network layer removes the IP header and forwards remaining message to transport layer. Transport layers gets UDP header along with UDP datagram which helps to get the data meant for the destination system.

4.2.5 IP Address vs Port Number :

- As we have seen when message reaches to the destination system from lower layers to above layers the header added by client side layers are detached and the related data is forwarded to the next level.
- As shown in the Fig. 4.2.4 the message contains IP address as 193.14.26.7 from which we are able to select machine having the same IP address in the network. On that specified system uses are able to select an application Port number from UDP header which is 13.

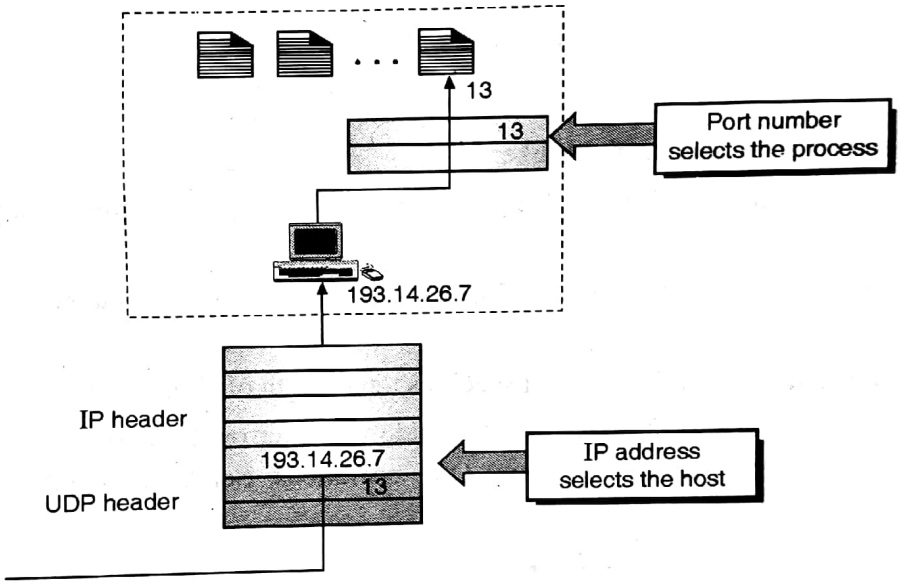


Fig. 4.2.4

4.2.6 Socket Addresses :

- It is a combination of IP address and port number.
- Socket address = IP address + Port number
  - **IP address** : It specifies the unique address of system in the network.
  - **Port number** : The specific number of any application which is running on the system.
- The socket address useful for running a particular application on the specified system which is specified by the socket address.

  For example as shown in the figure;

  IP Address: 200.23.56.8

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Port Number: 69

Socket address = 200.23.56.8 69

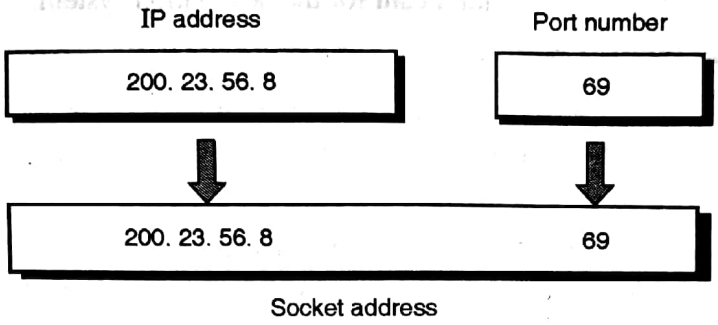


Fig. 4.2.5

4.2.7 UDP Datagram Format :

UDP datagram is of 8 bytes with various fields.

Header :

It has total 8 bytes and has fields like:

- **Source port number** 16 bits (2 Bytes):It indicates the port number of application on source system.
- **Destination port number** 16 bits (2 Bytes) :It indicates the port number of application on destination system.
- **Total Length** 16 bits (2 Bytes): It specifies total length of UDP datagram.
- **Checksum** 16 bits (2 Bytes) : It is helpful for error detection in the forwarded message with the help of AND and OR operations. Sender can decide whether to calculate checksum or not.

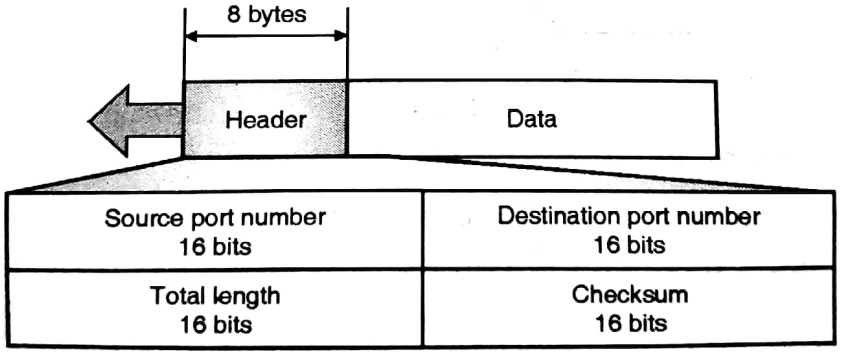


Fig. 4.2.6

4.2.8 Pseudo Header Added to UDP Datagram :

The UDP datagram along with the pseudo header is as shown in the Fig. 4.2.7.

- **Pseudo header :** It is added with UDP datagram header.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Source IP address :** 32 bits (4 Bytes)
  It indicates the IP address of source system.
- **Destination IP address :** 32 bits (4 Bytes)
  It indicates the IP address of destination system.
- **Protocol :** Is of 8 bits and mentioned with port number 17.
  It specifies the protocol used.
  If the checksum at destination side if he founds that the value is changed during the transmission then destination can directly discard the packet rather than forwarding to wrong application.
- **UDP Total Length** : 16 bit (2 Bytes)
  It is mentioned as specified below :
  UDP Length = IP Length – IP header Length

Header :

- It is made up of total 64 bits (8 Bytes).
- The fields are as mentioned above :
  - Source port number : 16 bits (2 Bytes)
  - Destination port number : 16 bits (2 Bytes)
  - Total Length : 16 bits (2 Bytes)
  - Checksum : 16 bits (2 Bytes)

Data :

- The data is added along with the pseudo header of 96 bits (12 bytes) and header of 64 bits (8 bytes).
- The padding is considered while data is mentioned in datagram, to make the data multiple of 16 bits.

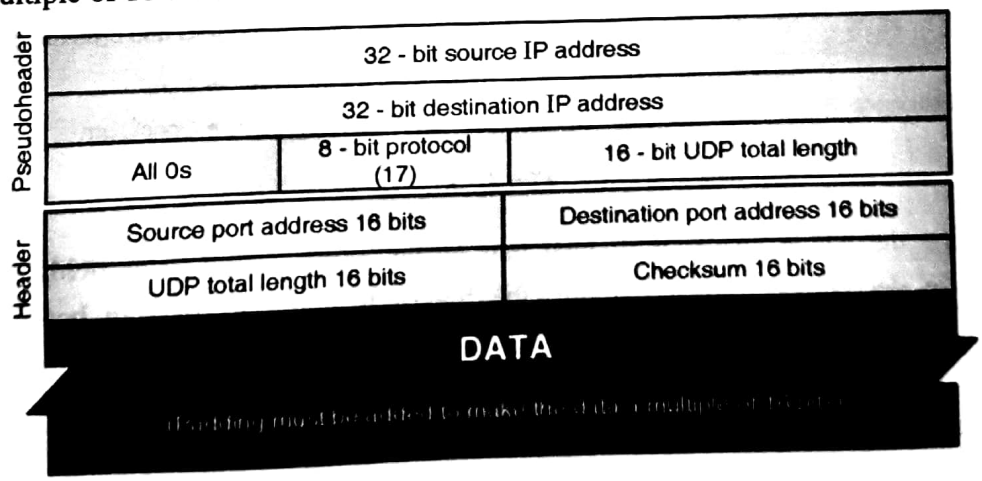


Fig. 4.2.7

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.2.9 Checksum Calculation :

The UDP header shown below in the decimal format.

In the example the mentioned fields are :

- **Source IP address :** 153.18.8.105
- **Destination IP address :** 171.2.14.10
- **Port number :** 17 (UDP port number)
- **Source port address :** 1087
- **Destination port address :** 13
- **UDP total length :** 15
- **Checksum :** All 16 bits of zeros
- **Data :** TESTING (mentioned with the ASCII code of characters) along with 8 bits of zero padding to adjust the 16 bit length.

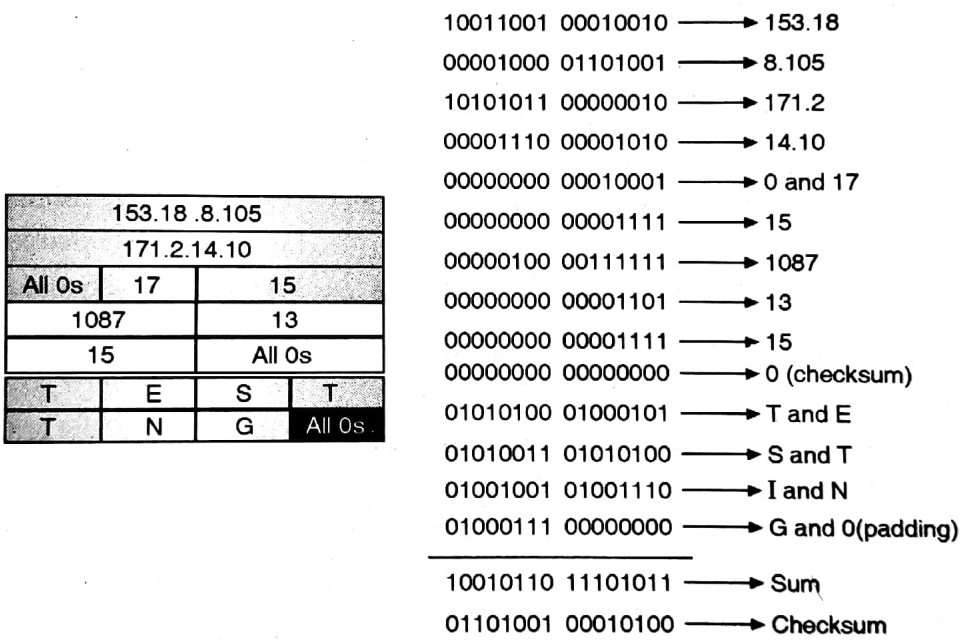


Fig. 4.2.8

At first the whole header is divided into 16 bit format. The header fields which are mentioned in decimal are converted into the binary format. The data in header is also mentioned with binary format along with padding if needed to make total length as 16 bits. Then all the binary bits are added by using ADD operation. Eventually the sum is displayed. Sender compliments the sum two times and finally the checksum is displayed.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.2.10 Encapsulation and Dencapsulation :

When source process wants to transmit message to destination process the following steps are followed :

(a) Encapsulation :

1. The client process sends message (UDP Data) from transport layer by adding UDP header.
2. Then in the network layer this whole data along with UDP header + UDP data is considered as IP data and on it IP header is attached.
3. Then it is forwarded to data link and physical layer where it is called as Frame data i.e. IP header + IP data. On this frame data frame header added by these lower layers and forwarded to the desired destination.
4. This process is called as "Encapsulation".

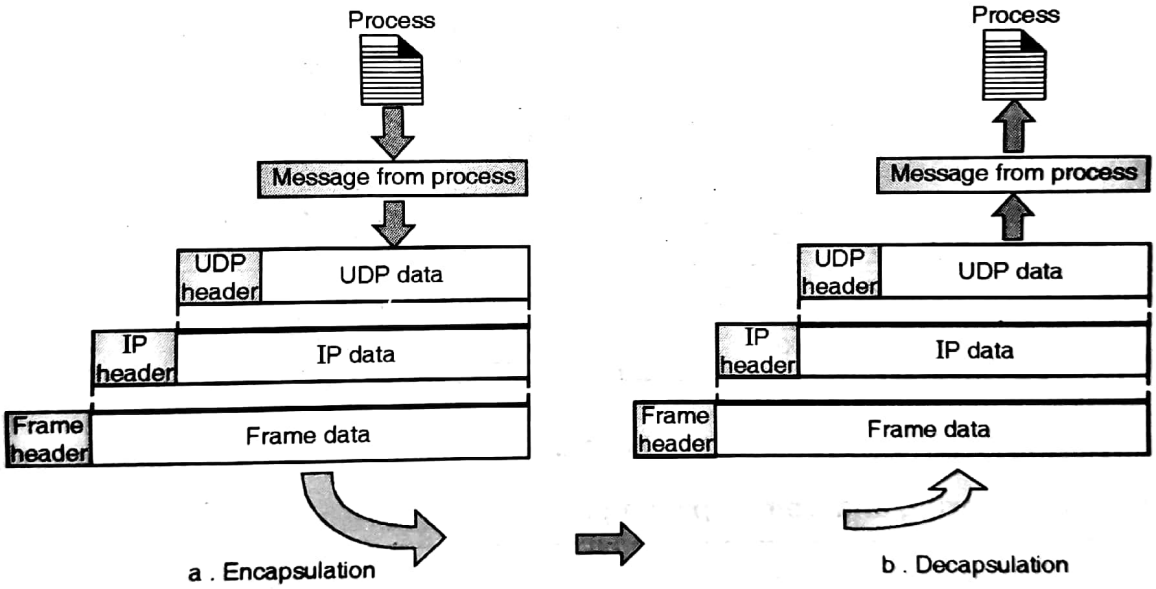


Fig. 4.2.9

(b) Dencapsulation :

1. The client process sends frame data along with frame header over the network to the destination.
2. The message is read by separating the frame data and the frame header by the data link and physical layer of OSI model.
3. Then the frame data forwarded to network layer where the IP header gets detached from IP data.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4. Finally when IP data reaches to transport layer process get the UDP data along with the UDP header.
5. The final message reaches to the destination process with only the needed information mentioned in UDP header and UDP data.
6. This process is called as "Dencapsulation".

4.2.11 Queue in UDP :

- As shown in the Fig. 4.2.10 there are two process queues maintained in UDP at client UDP and also at server side UDP. Client as well as server keeps; *outgoing* messages from the processes in the *outgoing* message storage queue.
- At the same time client as well as server keeps *incoming* messages from the processes in the *incoming message storage* queue.
- The UDP client port number 52000 and The UDP server port number 13 maintains both the queue for the smoothness in the transmission of UDP packets over the network and to avoid the congestion.

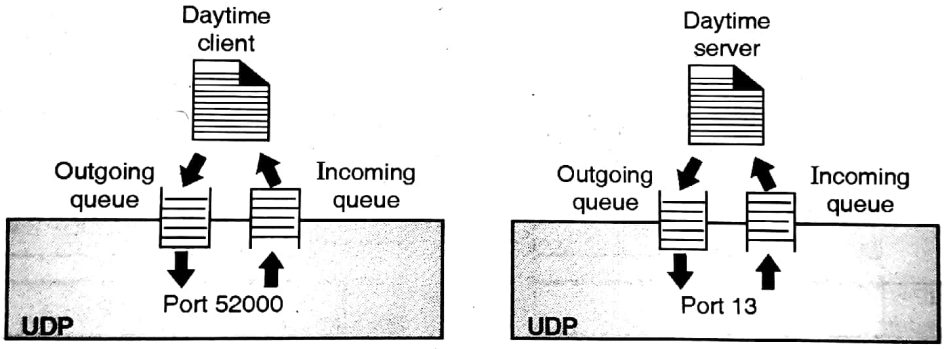


Fig. 4.2.10

4.2.12 Multiplexing and Demultiplexing :

(a) Multiplexing = Number of inputs only single output
(b) Demultiplexing = Single input only one output

(a) Multiplexing :

The client side works as multiplexing it means number of processes are given to UDP multiplexer and then only single output comes which is forwarded over the network layers at the destination side.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(b) Demultiplexing :

At the destination side when the packet reaches it specifies only one input but when passes through UDP demultiplexer it gives data to various processes as per mentioned in the particular datagram.

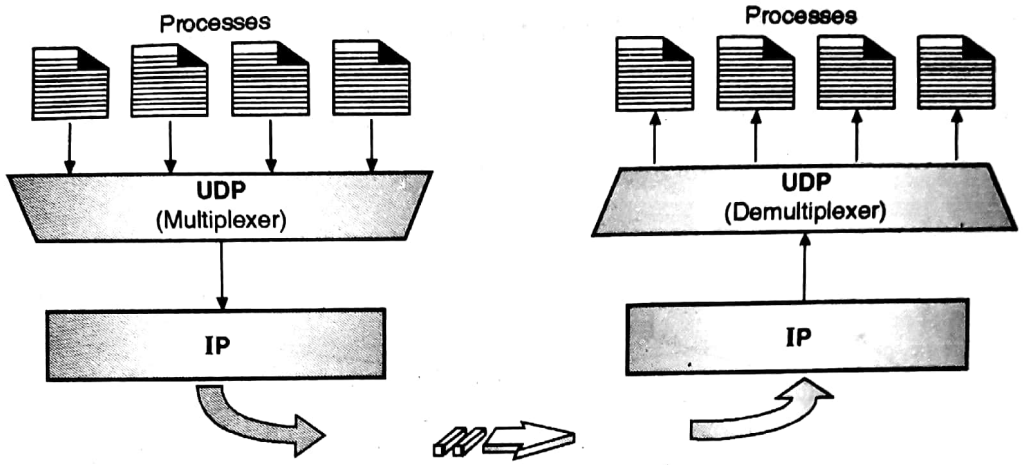


Fig. 4.2.11

4.2.13 UDP Package :

As shown in the Fig. 4.2.12 there are number of application processes working in the network. The UDP package contains the following different parts which are explained as follows ;

Input Queues :

In UDP there are number of input queues are mentioned which belongs to the specific process. There is no any output queue in UDP.

Control block table :

- It keeps the information about the ports.
- The details it specifies like;
  - The state of specific port like FREE or IN USE
  - The Process ID number
  - The port number
  - The queue number of specific process.

Control block module :

- It is mostly helps to control the control block table entries.
- When any new entry of a process should be added in table the incoming process first passes the process id and the port number (which is given by the operating system).

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- It does not create the new queues.

Input Module :

It receives user datagram from the IP layer and checks control block table weather any entry having same port number related with the incoming process.

- **If entry is available :** The module keep that data in the particular queue for the datagram.
- **If entry not available:** The module generates an ICMP error message like "Port not Found", "unable to reach port", "queue does not exists".

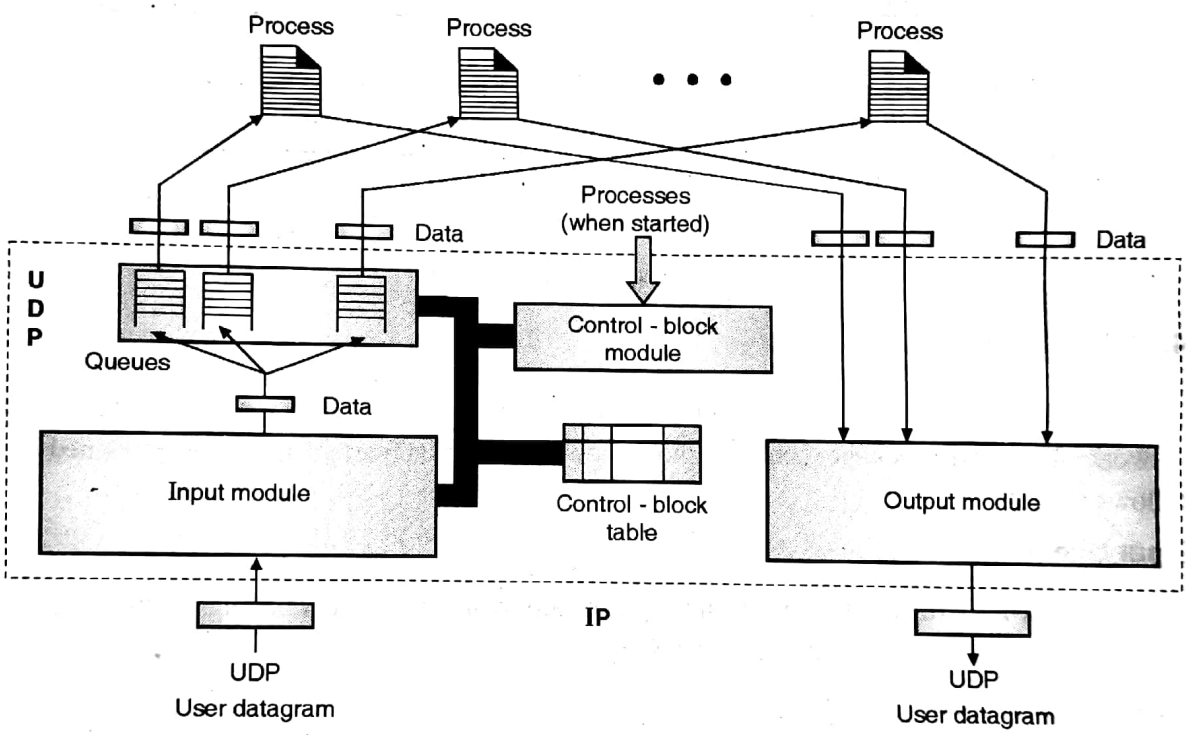


Fig. 4.2.12

Output Module :

It is helpful for sending user datagrams to the IP layer generated by various processes.

4.2.14 UDP Application :

- UDP is useful for simple applications between client and server.
- It is beneficial when the process are internally having the error control and flow control capacities.
- UDP is useful in network management protocol like SNMP.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.2.15 UDP Service Issues :

- UDP is totally message oriented protocol.
- It is known as connectionless protocol since without prior established connection data/ message is transferred over the network. There is no any relationship between datagram send from same user.
- UDP most of the times delivers exact message or if any issue occurred while transmission then it does not deliver the packets(datagrams).
- The sequence of datagram is not followed in the UDP.
- As the path discovered, the datagram is forwarded. Several messages are delivered in the network at the same time via different paths available in the network.
- Due to this if any route is short then the datagram forwarded using that route will reach destination fast.
- Hence the datagrams reaches to the destination in the disorder.

4.2.16 Error Control :

- While transferring the message over the network it may be lost, that time an application must report loss recovery.
- If a UDP message having size larger than (MTU) Maximum Transfer Unit, then fragmentation takes place at the IP layer.
- As we have seen the maximum size of message is 8 K Bytes.

4.2.17 Flow Control :

It does not provide flow control mechanism hence the congestion occurs in the network while transmission of large number of datagrams.

Solution :

- Due to some issues in UDP i.e. User Datagram Protocol we use TCP (Transmission Control Protocol).
- TCP helps to overcome the pitfalls occurs in UDP transmission as well as it helps for handling issues like Error correction, Flow control and Congestion control in the network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3 Transmission Control Protocol (TCP)

4.3.1 Position in OSI Layer :

The TCP (Transmission Control Protocol) is a transport layer protocol which is helpful for allowing congestion free, error less and flow controlled transmission of data segment over the network.

- TCP is connection oriented protocol. It means when sender wants to transfer data segment to the receiver the connection between them should be established.
- The connection is established with the help of commands and acknowledgement to that commands by both the sides which are connected.
- It transfer the segments in the sequential manner by following the same path.

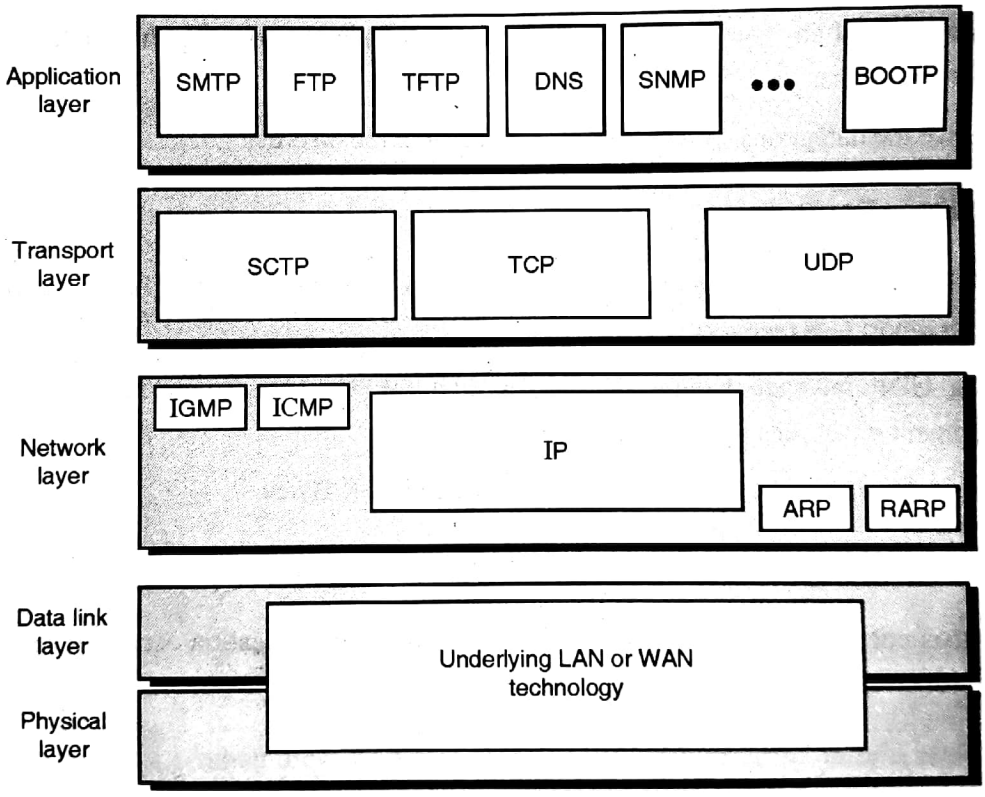


Fig. 4.3.1

4.3.2 Error Control :

TCP also provides provision of retransmission of segment if it is lost in between the network or if sender does not get the acknowledged for that.

Using TCP sender can send large amount of data over the network by considering specific packets or segments.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3.3 Flow Control :

It helps to control the transmission of segments between sender and receiver by using buffers. It controls the speed of transmission of segments between sender and receiver.

4.3.4 Well-known Protocols in TCP along with the Port Numbers :

- SMTP (Simple Mail Transfer Protocol) - 25

  Useful for electronic mail transfer over the network

- TELNET (Terminal Network) - 23

  Helps in remote transmission over the network.

- DNS (Domain Name system) - 53

  Useful while specifying domain of particular site

FTP (File Transfer Protocol) :

- For data- 20

  For data transmission between client and server

- For control - 21

  For controlling data transmission between client side and server side.

  HTTP (Hyper Text Transfer Protocol) - 80

  For transferring web documents between the Internet users

4.3.5 Stream of Delivery :

- The TCP is not like UDP datagram which helps to transfer max 8KB data over the network.
- TCP transfers stream of data between client and server as shown in the Fig. 4.3.2.

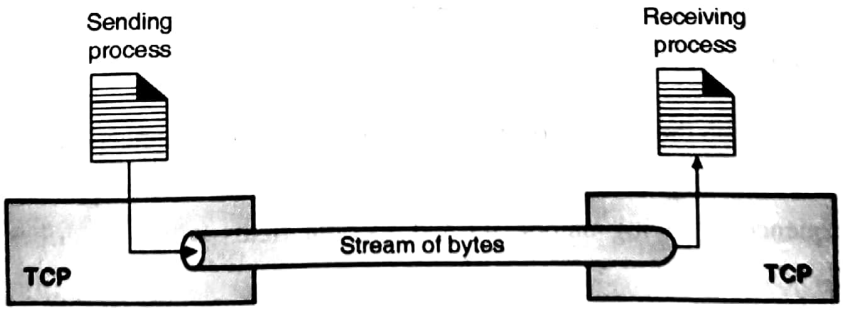


Fig. 4.3.2

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3.6 Sending and Receiving Buffer :

Working on Stream of data:

- In TCP there are two ends like Sending process and Receiving process.
- Since by using TCP, sender able to send stream of data to the receiving process but if the sender is fast and the receiver is slow or sender is slow and the receiver is fast then the transmission gets affected.
- To maintain the communication smoother between both the ends the stream should be transfer properly from client to server.
- The speed of transmission should be decided as such there should not occur any congestion or overhead on the receiver's side.
    - **Requirement of buffers :** Since we want to maintain the smooth communication between users the data stream should be stored in the buffer.
    - **Sender's buffer :** When sender generates the data stream for transmission it keeps on adding data in its buffer.
    - **Receiver's buffer :** At the receiver's end the stream is forwarded and buffered ; whenever receiver process requires the data it can access it or retrieve it from the buffer.
- The bytes of data to be consider in the data stream is totally dependent on the TCP. The data stream length is randomly decided.

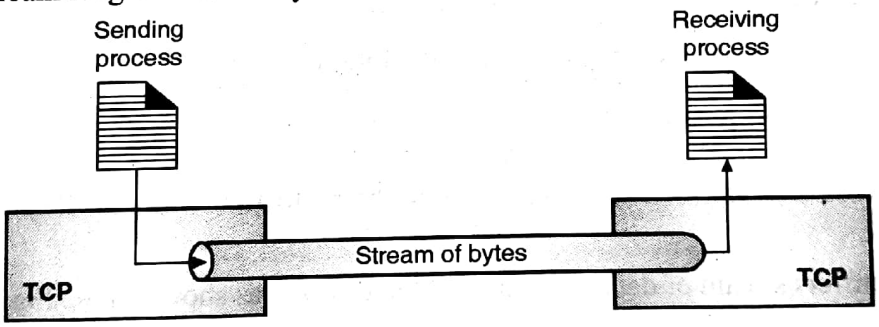


Fig. 4.3.3

4.3.7 TCP Working :

- The TCP transfers the number of bytes as a stream over the connection as a segment.
- It can transfer number of segments which are having number of bytes.
- Each sequence is having unique ID and specific fields which describes the segment properly.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

For example :

- If one TCP connection transferring file of 3000 bytes then what will be the details of following 3 segment if segment is carrying the 1000 bytes.
  - **Segment 1 :**

    Sequence No : 12001 (range 12001 to 13000)
  - **Segment 2 :**

    Sequence No : 13001(range 13001 to 14000)
  - **Segment 3 :**

    Sequence No : 14001(range 14001 to 15000)

4.3.8 TCP Segment Format :

The TCP segment is made up of various fields.

(a) Source Port address : 16 bits (2 Bytes)

It specifies the port address of process running on the source system.

(b) Destination Port address :16 bits (2 Bytes)

It specifies the port address of process running on the destination system.

(c) Sequence Number : 32 bits (4 Bytes)

It specifies the unique sequence number of the segment. It describes the number of first data byte in the segment. Due to unique number we are able to discriminate the segments.

(d) Acknowledgement Number : 32 bits (4 Bytes)

It gives an acknowledgement send by both sender as well as receiver as a positive reply along with the next expected segment's sequence number.

(e) HLEN : 4 bits

It specifies the header length of a segment.

(f) Reserved: 6 bits

It contains total 6 bits which are stored for the future purpose

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(g) Control fields : 6 bits

It describes the details or the purpose of the segment with six different types.

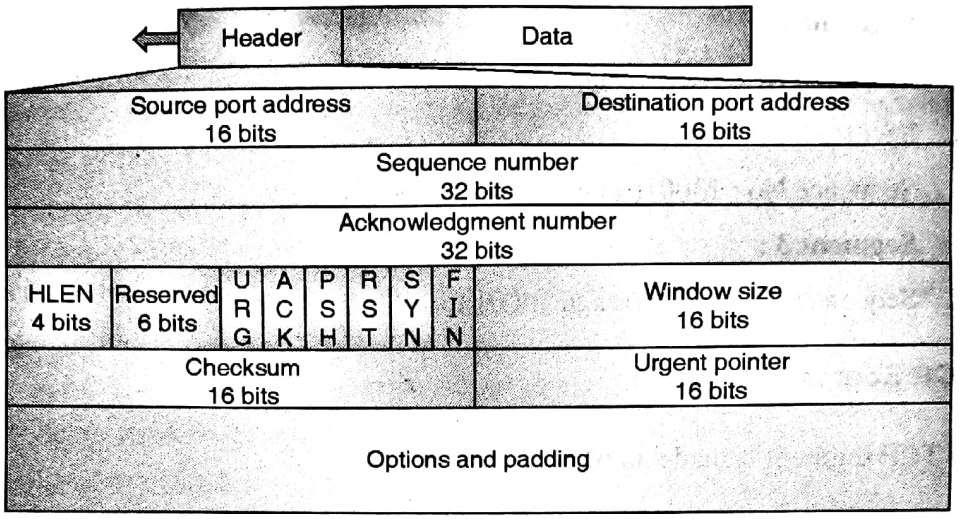


Fig. 4.3.4 : TCP segment

(h) Control Field :

1. **URG : (Urgent Pointer)**

   It helps to specify that the current segment lies in urgent category. It means it is required to be considered as soon as possible for the further operations.

2. **ACK : (Acknowledgement flag)**

   - It specifies that current segment is acknowledged by the sender or receiver and also the next sequence number is included in segment.
   - The segment having the acknowledgement number if does not carrying any data than sequence number is not mentioned in the segment

3. **PSH : (PUSH at the receiver's side)**

   It specifies that data is pushed in the receiver's queue.

4. **RST : (RESET the connection)**

   It explain that the whole transmission is reset and the segments are transferred again by reseting the connection between sender and receiver.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

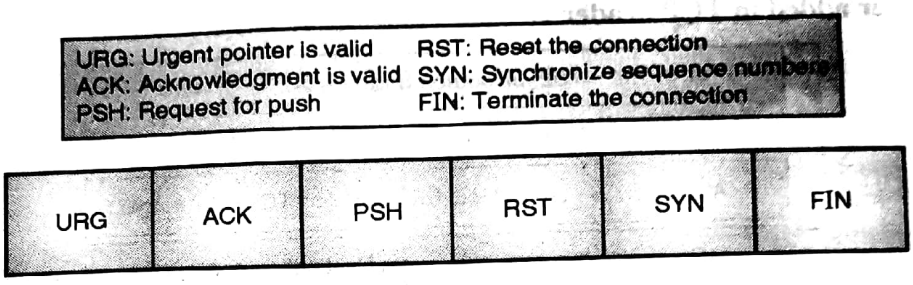


Fig. 4.3.5

5. **SYN : (Synchronize the sequence numbers of segments)**

   It describes that the segment with unique sequence number which are transferred between sender and receiver.

6. **FIN : (Finishing or termination of connection)**

   This flag is used when sender wants to close the transmission of segments i.e. while finishing the data transfer from sender the sender passes segment which enables the FIN tag.

(i) Window size : 16 bits (2 Bytes)

- It specifies the maximum size of the segment to be send.
- If sender sends the segment in which particular segment size is mentioned called that as receiver's window size.
- It means the receiver not suppose to send any segment which carrying data size more than the limit specified by the sender previously same rule is applicable for the receiver to sender sending.

(j) Checksum :16 bits (2 Bytes)

In TCP checksum plays an important role. It helps to detect an error in the transferred data.

(k) Urgent pointer : 16 bits (2 Bytes)

If the URG flag is enable than the urgent field contains some data which is necessary to transfer over the network.

(l) Data and Options :

The data is added with the padding to make it suitable to 16 bit data

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Pseudo header added in TCP header :

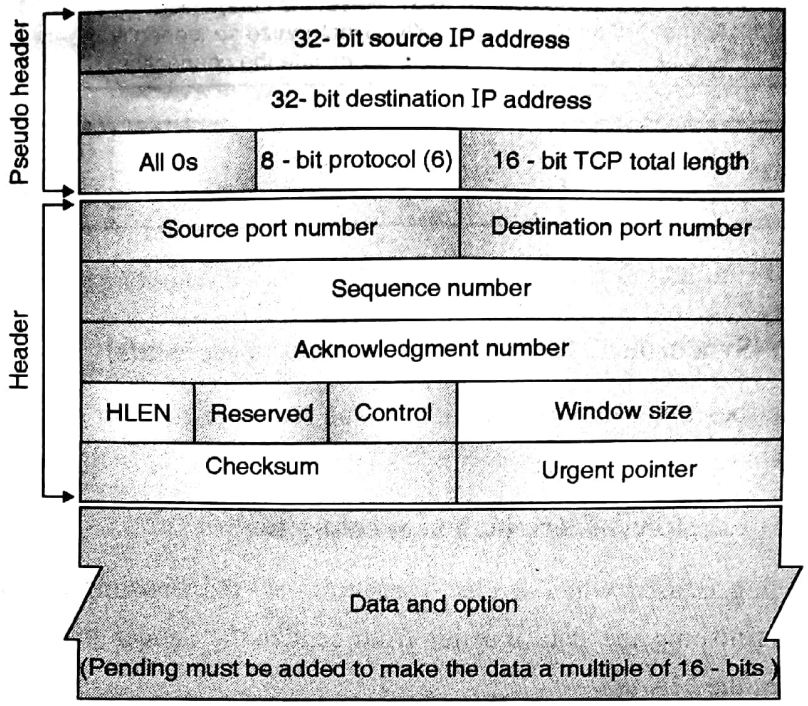


Fig. 4.3.6 : Psedo header in TCP header

4.3.9 Encapsulation and Dencapsulation :

Frame header	IP header	TCP Segment

- At the time of transferring data over the network for the security purpose the encapsulation and dencapsulation is done with the data.
- The TCP segment is send from client by following network layer, physical layer.
- Then transferred over the web and given that data to receiver's side.

(a) Encapsulation :

The segment which we want to transfer from client to server is encapsulated by network layer using IP header and then by lower layers by frame header.

(b) Dencapsulation :

- Data which comes from the network is given to lower layers of OSI layers at the server side and while forwarding it the detachment of header by individual layers takes place.
- This process is called dencapsultion.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3.10 TCP Connection :

Q. A TCP connection is in ESTABLISHED. The following events occur one after another.

(a) A FIN segment is received

(b) The application sends a "close" message. MU - April 2013

Since TCP is connection oriented while doing the transmission between sender and receiver the connection must be established prior to the transmission.

TCP deals with the following connections while the transmission of segments :

- Connection Establishment
- Data Transfer
- Connection Termination
- Connection Reset

(a) Connection establishment using 3 way hand shaking :

As shown in the Fig. 4.3.7 the client and server establishes connection using three messaged hence it is known as "Three way handshaking".

1. First client active opens the connection and passes the SYN segment towards the server.

   The segment contains details like:

   - Initial Sequence Number(ISN) which does not contain any real data just a byte is considered and it is any random number.
   - It does not specify any window size since it is not transferring any acknowledgment.

2. Server passive opens the link and forwards the segment containing SYN + ACK

   In this case the segment send by server contains details like;

   - It increments the sequence number of segment by 1 and indicates that data transfer started.
   - It specifies an acknowledgment of previous segment and also specifies the sequence number of next expected segment.
   - Since it contains the ACK the receive window size need to be specified which indicates the maximum size of data can be send from the client's side.
   - It specifies both the SYN and ACK flags.

   It is again one ACK segment. Along with ACK flag.

   - It usually does not carry any data.
   - It specifies the window size for the server side.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- It contains same sequence number as per the previous segment.
- Finally the connection is established between client side and server side systems.

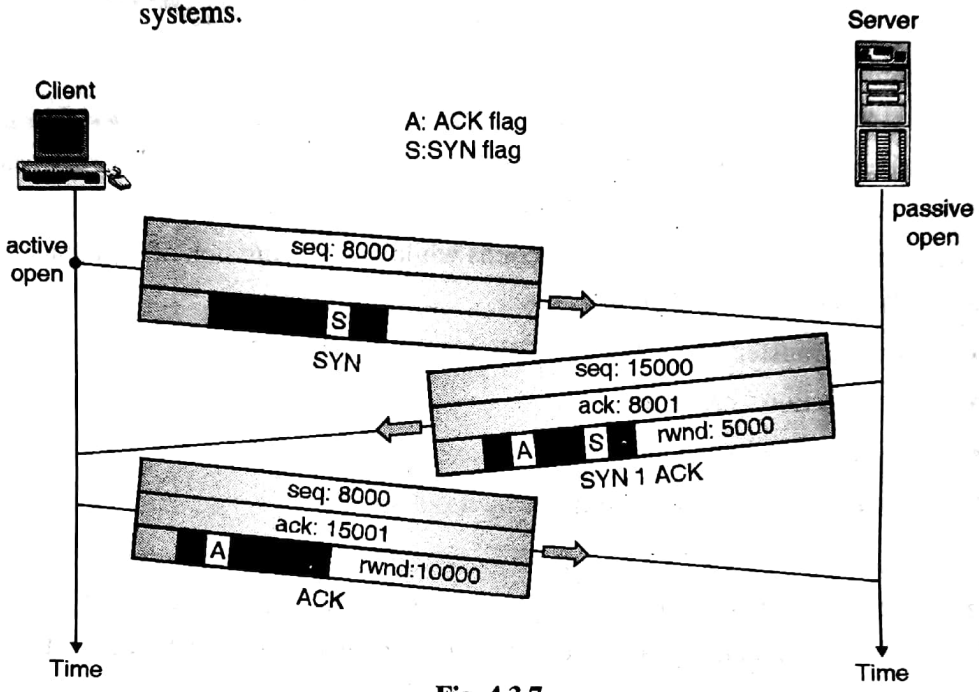


Fig. 4.3.7

SYN flooding attack :

1. In the client server connection TCP follows three way hand shake protocol.
2. Whenever client send SYN to the server as reply server sends acknowledgement (ACK) to that SYN.
3. When client get a SYN + ACK it sends ACK and the connection between both the end is established.
4. If in the network one server gets number of SYN from various clients and in the small period then server gets overloaded.
5. The server not able to recognize whether all the clients are real.
6. Due to fake clients which sends number of SYN rapidly to server showing that it is from different IP addresses and server then allocates the resources to them without any authentication.
7. Finally server not able to serve any client due to lack of resources and congestion.
8. Sender replies to the SYN but since number of addresses are fake it does not get any ACK.
9. This situation is known as " SYN flooding attack".

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

10. And due to such type of scenario real client those who belongs to network does not get services from server it is called as " denial of service attack".Server not able to provide services to the valid clients.

(b) Data Transfer :

- After the successful completion of three way handshake connection.
- The sender starts sending the segments with the full information about the various fields.
- There are two segments of 1000 bytes each are transferred to the receiver's side. The two segments which contains the following details like :

Segment 1 :

- Sequence number : 8001
- acknowledgement number : 15001
- enable control flags : ACK and PSH
- Data bytes : 8001 – 9000

Segment 2 :

- Sequence number : 9001
- acknowledgement number : 15001
- enable control flags : ACK and PSH
- Data bytes : 9001 – 10000

- The sequence number specifies unique id of the segment.
- Acknowledgement number specifies what is starting number of next data byte.
- Control fields ACK and PSH is mentioned to specify that the data transmission has been started between client and receiver; and the data bytes are pushed in the receiver's buffer.
- The receiver sends back the reply to the sender with one segment containing 2000 bytes.

Segment 1 :

- Sequence number : 15001
- Acknowledgement number : 10001
- Control field : ACK of next data type.
- Data bytes : 15001 – 17000

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

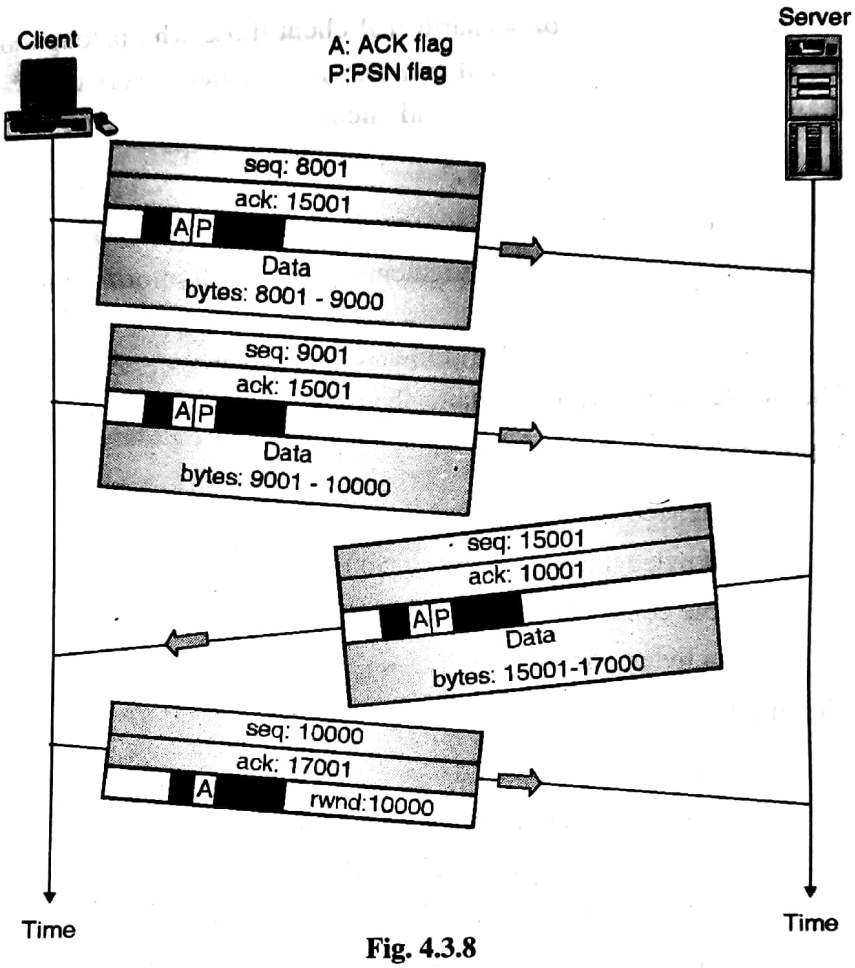


Fig. 4.3.8

c) Connection termination :

- When sender wants to terminate the connection it actively close the connection by sending FIN enabled segment.
- Then receiver sends back ack + FYN to specify that it has done passive close.
- Finally sender sends ack segment which terminates the connection between sender and receiver.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

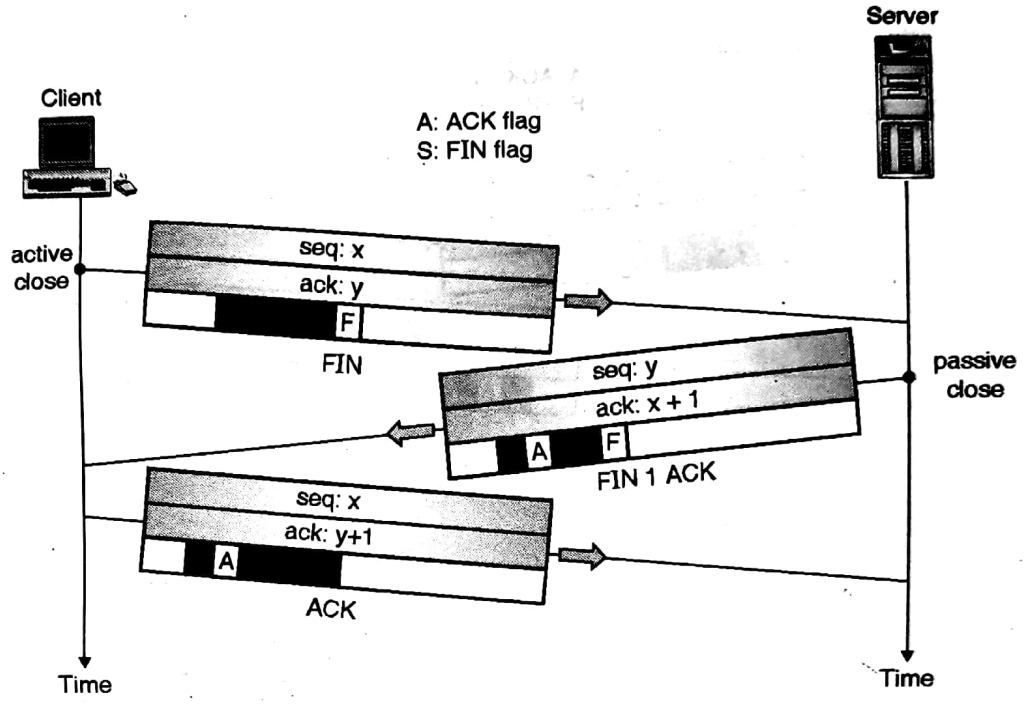


Fig. 4.3.9

d) Half Closed :

- If in between the transmission sender specifies active close by sending FIN segment.
- Receiver replies with ack segment that receiver got the message about termination of the connection.
- Receiver transfers the remaining data to the sender and even sender replies with the acknowledgement to receiver.
- After completion of these data transfer the receiver passively close the connection. And then final ack comes from the sender about termination of the connection.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

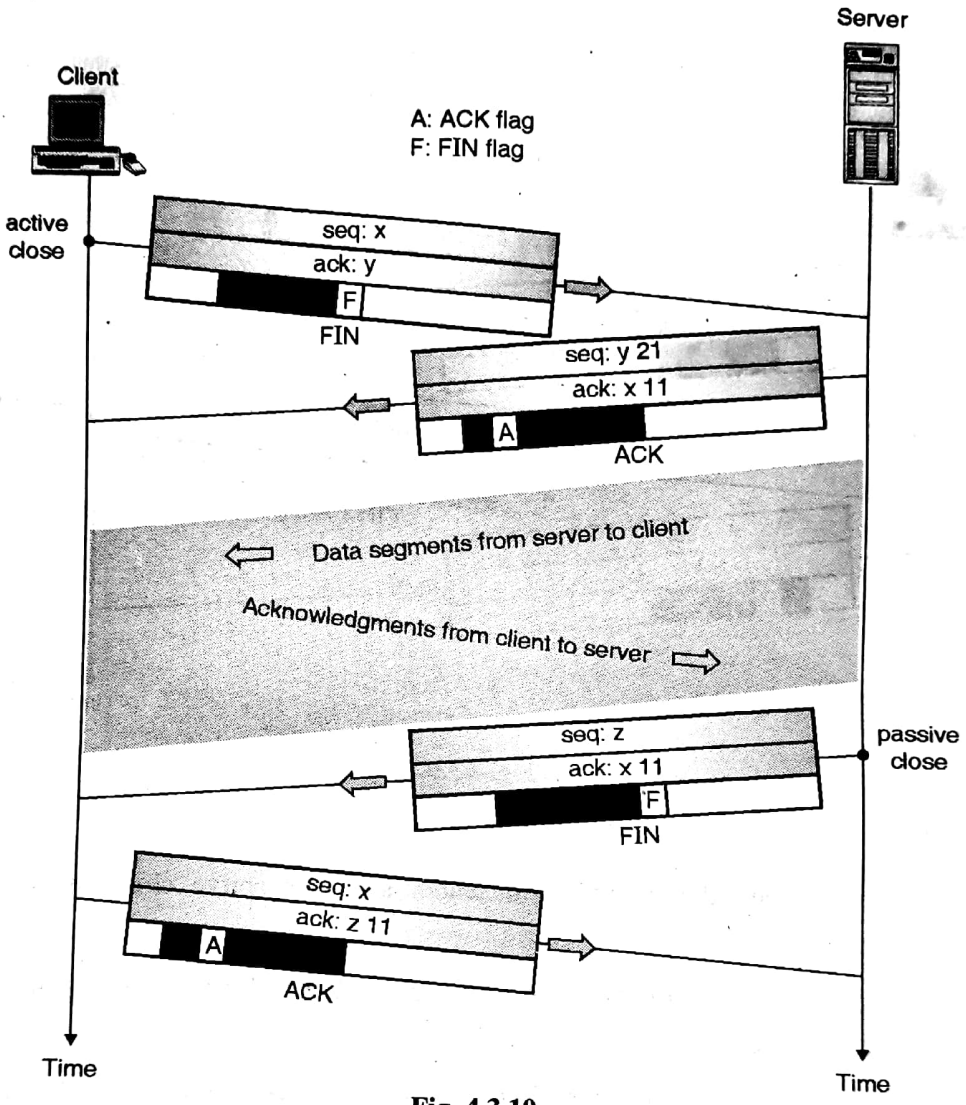


Fig. 4.3.10

4.3.11 States of TCP :

States of TCP segments are mentioned below:

(a) Closed :

Still there is no connection between sender and receiver.

(b) Listen and SYN SENT :

Sender does passive open and sends SYN to the receiver and waits for ack from receiver's side.

(c) SYN RCVD :

Sender sends SYN + ACK and waits for the ACK from receiver.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(d) Established :

Connection established between sender and receiver now data transfer can takes place.

(e) FIN Wait-1 and FIN Wait-2 :

- First FIN send by sender and waits for ack from receiver
- Sender receives ACK of first FIN and waits for reply for second FIN ACK from receiver.

(f) Close wait :

Since first FIN ack is received waiting for application to close from the receiver's side.

(g) Time Wait and Last Ack :

Second FIN received by the receiver and waiting for ack till the time period of 2MSL (Maximum Segment Length)

(h) Closing :

After the ack of last FIN both side simultaneously close the connection

4.3.12 State Transition Diagram :

In the Fig. 4.3.11

- Ovels : Mentions the states
- Lines : Describes the transition from one state to other.
- Slashed data : The first string represents the data received by the TCP and second string represents data send by TCP.
- Solid lines : State change of server
- Dotted lines : State change of client.
- Established : Is state of connection establishment between client and server.
- MSL : Maximum segment length is mostly considered between 30 seconds to 1 minute.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

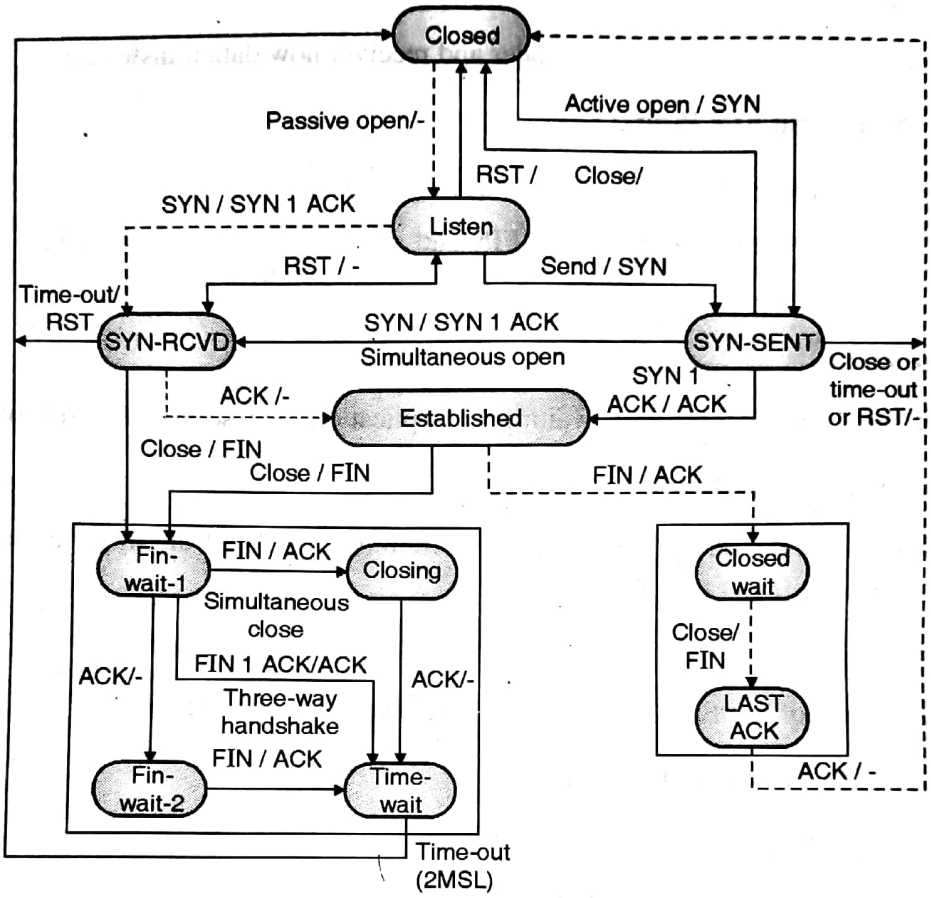


Fig. 4.3.11

4.3.13 Some Connection Scenario :

(a) Connection established and Half closed :

- Client : active opens and active close the connection
- Server : passive opens and passive close the connection

Client states :

- The client *active opens* the connection.
- It sends *SYN* segment to server and waits for the acknowledgement for the SYN segment
- After getting *ack of SYN* sender sends acknowledged segment back to server.
- Finally the *connection is established* between client and server and then data transmission starts.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- After the completion of data transmission client active close the connection by sending the *first FIN* and waits for acknowledgement from server.
- When *ack of first FIN* is received client wait for finishing the data transmission from server side. It also sends ack for received data and waits for second FIN from server.
- Whenever client gets *second FIN* from server it sends back acknowledged
- After waiting for 2MSL (Maximum Segment Length) time out takes place and the connection is *closed* from client side.

Server States :

- Server *passive opens* the connection and listen for the SYN from client side.
- When *SYN – RECVD* is started after getting SYN from the client.
- Then server sends *SYN + ACK* as an reply for SYN from client which represents the server is ready for connection.
- After getting the *ack* the connection is *established* between client and server.
- Then data transmission starts between client and server.
- When server gets *FIN from client* it informs to the server process about active close from client.
- Then sends *ACK of FIN to* the client.
- Till data transmission is occurring between client and server it ***Close wait*** for sending *second FIN* till data transmission is getting over.
- Then waits for the *Last ack* from client
- After getting an ack for second FIN connection is *closed.*

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

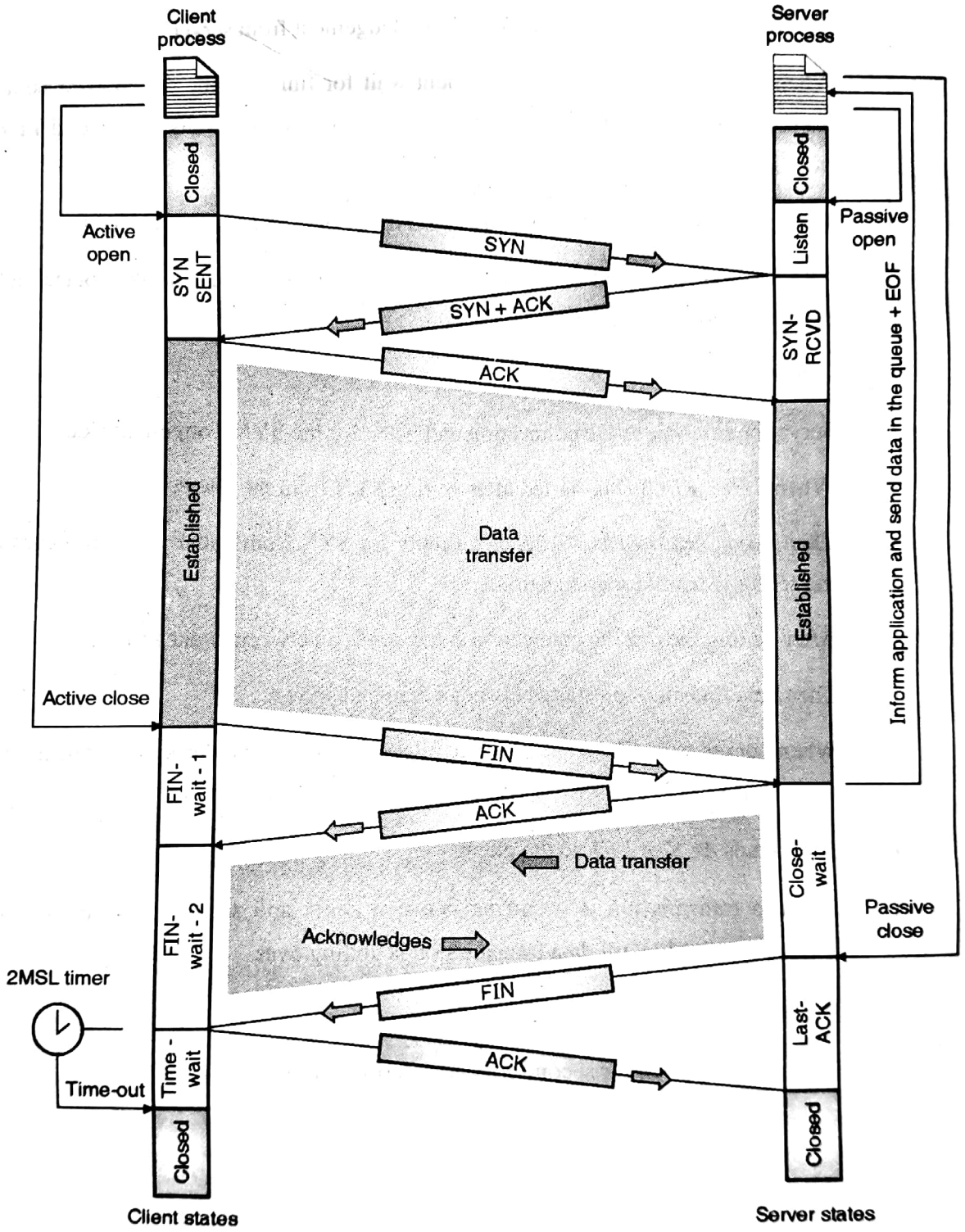


Fig. 4.3.12

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(b) Simultaneous Open and Simultaneous Close :

Simultaneous Open :

As shown in the figure;

- Both the processes sends SYN message to each other at the same time for establishing the connection between them.
- If both the processes gets back an acknowledgement i.e. ACK + SYN then the connection establishes between them.

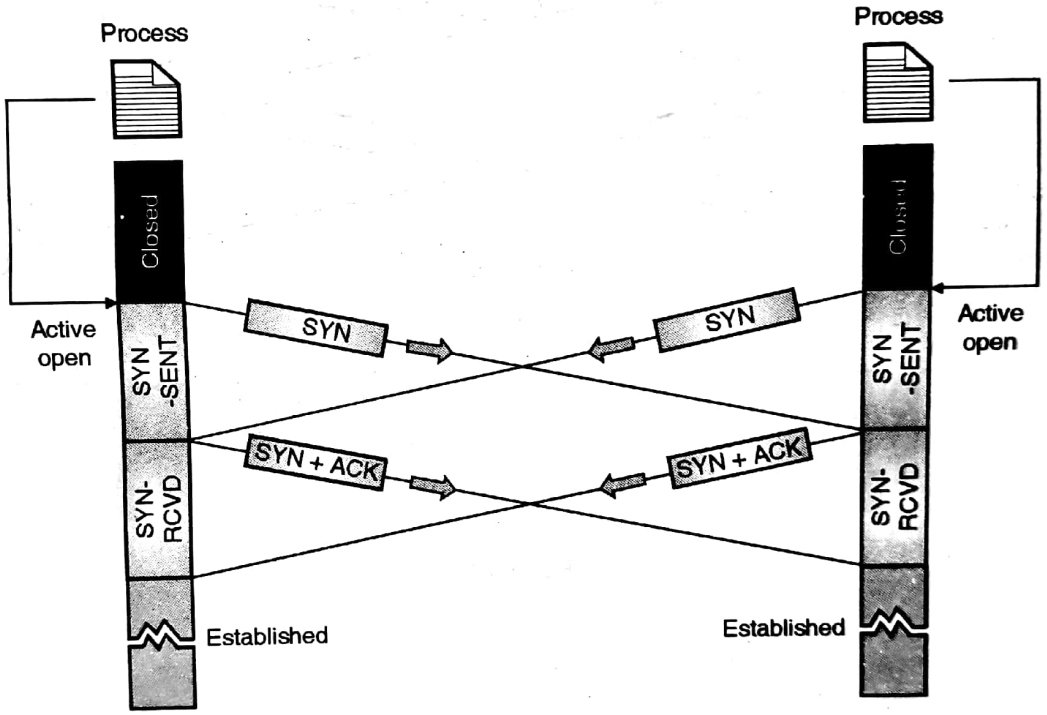


Fig. 4.3.13

Simultaneous Close :

- In the network if two processes are working for termination of connection at the same time than both sends each other a FYN flag.
- FYN specifies the termination of connection.
- When both processes sends back an ack flag.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

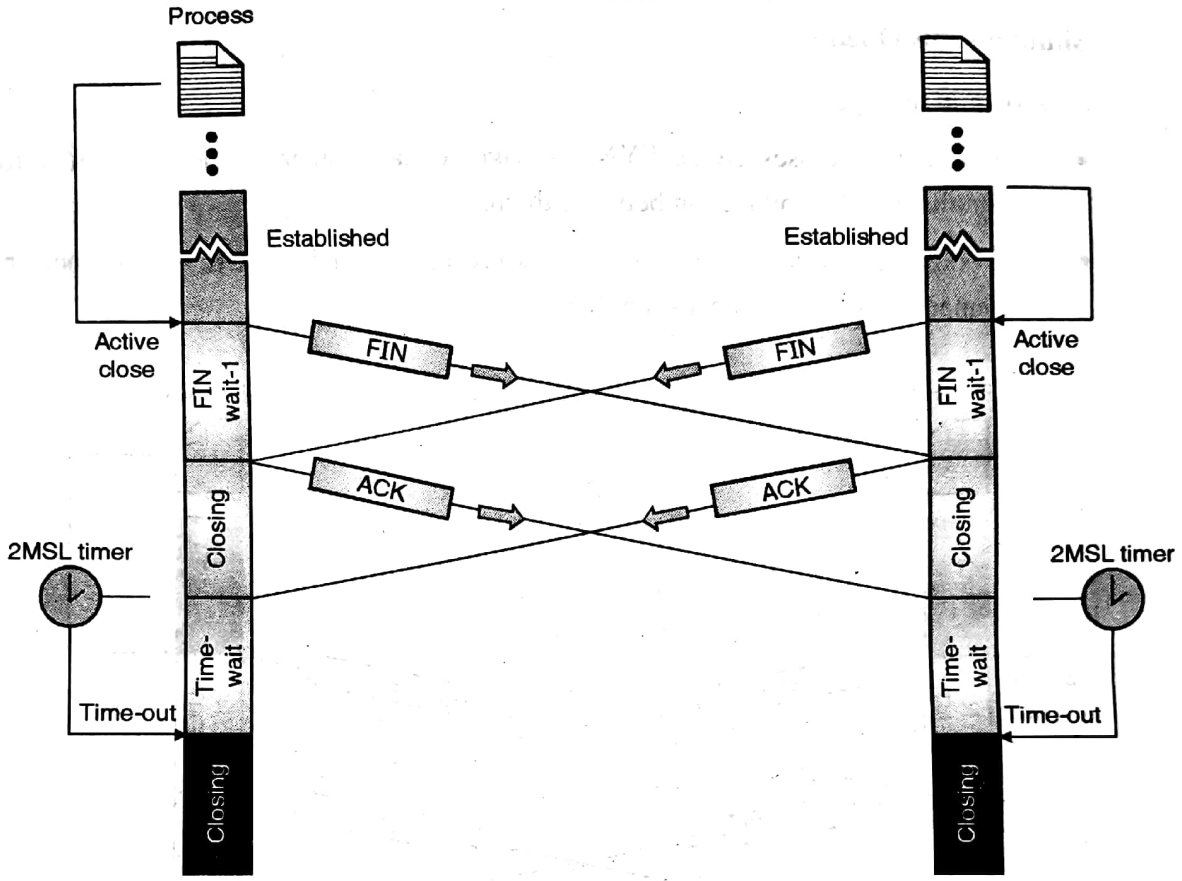


Fig. 4.3.14

(c) Denying Connection :

- As we have seen when client wants to send data to particular server it sends a SYN to server.
- If server is not ready ; server sends segment along with the **RST and ACK** enabled control fields to the client which tells client to reset the connection.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

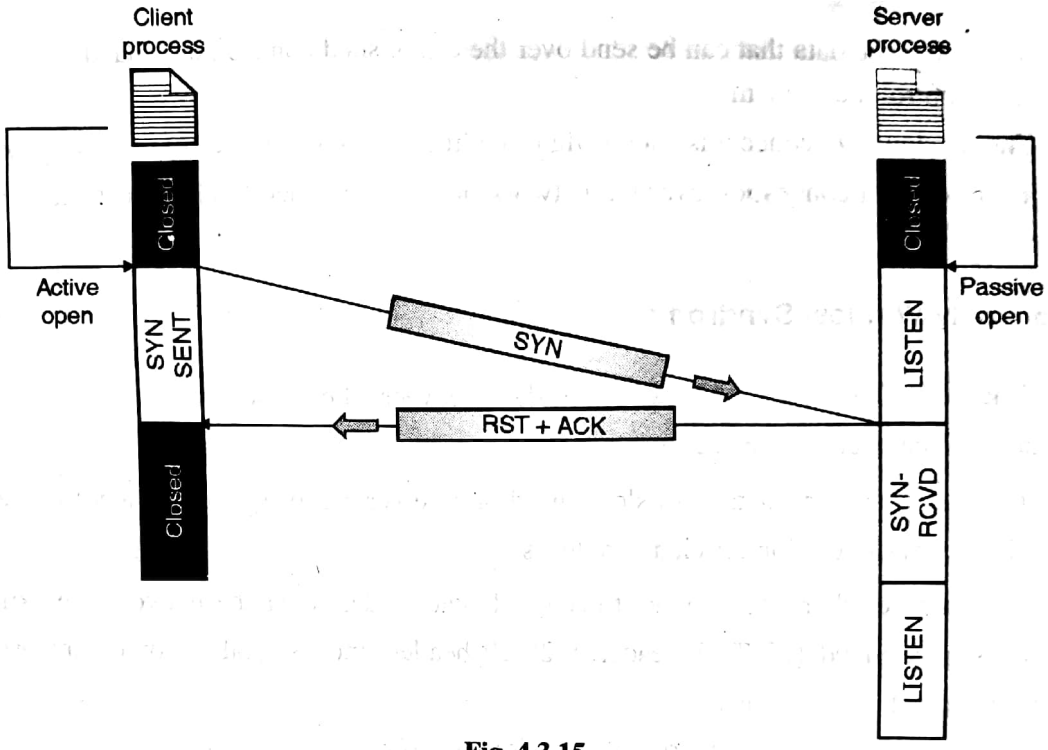


Fig. 4.3.15

(d) Aborting Connection :

- When the connection is established between client and server side if there exists any problem at the client process abort state occurs.
- Client sends RST + ACK i.e. reset connection is required between client and server.

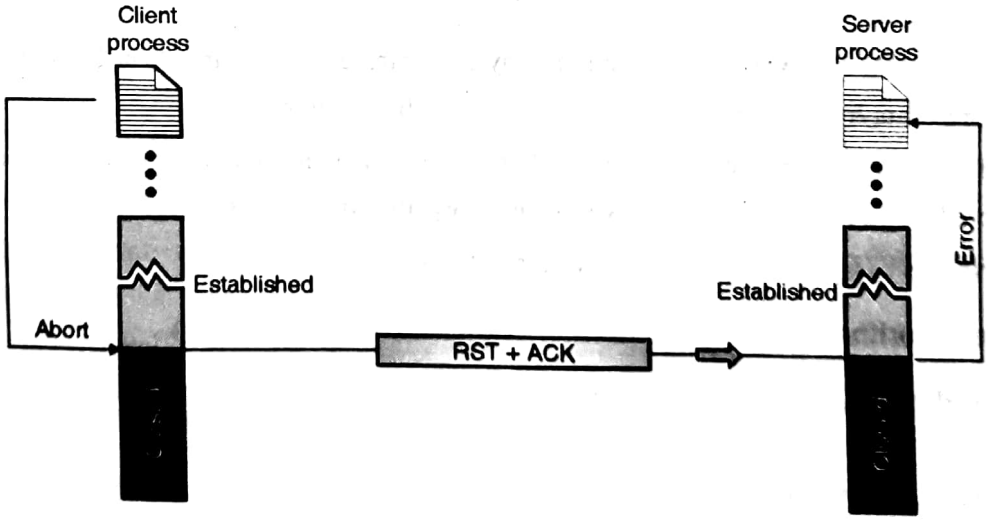


Fig. 4.3.16

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3.14 Flow Control :

- To control the data that can be send over the established connection is handled by using flow control mechanism.
- The window size concept is added while sending the data over the connection.
- To avoid data congestion over the network buffers are added to client as well as server side.

4.3.15 Silly Window Syndrome :

- When the TCP connection has established between client and server the data transfer takes place over the connection.
- If sender is sending data with slow speed or receiver receiving data slowly than due to this network operation efficiency reduces.
- For example when user wanted to send o1 byte of data over the network the extra 40 bytes gets added (20 TCP header + 20 IP header) means total 41 bytes are used to transfer just 1 byte of data.
- From this we can see the inefficient use of connection.
- This issue is known as "silly window syndrome" it is generated by both sender and receiver.

Syndrome generated by Sender :

- When in the network a client who generates 1 byte of data at a time create silly window syndrome.
- Due to this if over the connection 1 byte is transfered regularly than for transferring large data from same client takes number of 41 bytes segments.
- To avoid this inefficiency sender should keep data in its outgoing buffer for some predefined timer and transfer over the network after timer expires.
- Negle's has given some steps to avoid syndrome at client side.

Negle's Algorithm:

Sender in TCP sends first data as 1 byte to the server to check for availability of proper connection

1. Then after 1st byte now sender consider predefined timer to save data bytes in outgoing buffer of client.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2. The data bytes are send over the network when ;
   - Server sends an acknowledgement to previous data byte or
   - The maximum window size of sender gets full.
3. Same process is followed for other segments like if acknowledgement of segment 2 is received by client then it is able to send segment 3 or else if the maximum size in segment is achieved.

Syndrome generated by receiver :

- When sender is generating a data with the rate of some kilo bytes and receiver is receiving data with rate of bytes. Since receiver is slow the syndrome is generated by receiver.
- If sender sending number of bytes over the connection but receiver is not able to receive it with the same speed as it is generated.
- It means the receiver access data bytes from the sender in slow speed.
- For example sender sending data with 1 kbytes and receiver excepting data with 1 bytes at a time.
- The maximum size of receivers window is 4 kbytes.
- When the receivers window gets full it sends window size to sender as Zero.
- After the utilization of data from the buffer the receiver sends the ack with new window size.
- If the 1byte of window size gets free than receiver sends the acknowledgement along with the window size as 1 byte.
- And now the sender can send next 1byte of data to receiver.
- Due to this again transfer of 1byte of segments get started which is inefficient way of operation.

The solutions as follows :

Delayed acknowledgement :

- The receivers acknowledgements are delayed until there is some proper amount of window size is generated.
- It reduces traffic of small data segments transmission over the network.
- The delayed acknowledgment period is considered as not more than 500 ms.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

4.3.16 Sliding Window :

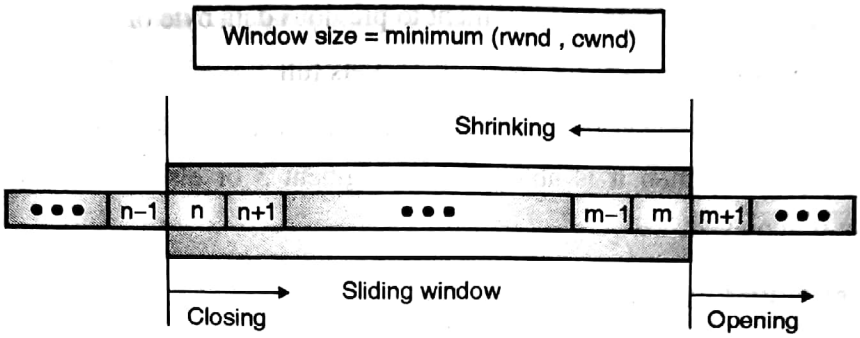


Fig. 4.3.17

- A sliding window concept is added to avoid the burden on the destination side and also to get an efficient transmission of data between client and server.
- Sliding windows considers data in bytes.
- The size of the window is the less than the receiver's window and congestion window.
- The sender does not sent full data at the one time.
- Window is handled by receiver to do any kind of operation.
- Destination also sends acknowledgement segment till the window does not shrinks

4.3.17 Error Control :

TCP is reliable protocol which provides some error control mechanisms as explained below:

- It detects corrupted, lost, out-of-order, and duplicated segments.
- Error control can be handled by TCP as
  - **Checksum :** To detect the error in the segment transferred over the network.
  - **Acknowledgement segment :** Ack segment does not contains sequence number and are not acknowledged by sender or receiver.
  - **Time-out :** After particular time slot still if the segment is not delivered than the error is occurred and to avoid this timer is set from sending event of any packet.
  - **Retransmission :**The retransmission of segments takes place when there is any error occur and wants to send back the lost segment after the expiration of timer The retransmission of ack segment is does not depends upon the timer.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(a) Lost Segment :

- Whenever the receiver sends a segment which contains requirement of the next data segment from the client.
- Sender sends the segment and at the same time it starts the timer.
- If while transmission the data segment gets lost in between than the gap is generated in the receiver's side buffer since data segment next to the current segment are forwarded.
- Since receiver does not get the required segment than it sends ack again and again to the sender.
- Than after the time out the sender resends the segment to the receiver.

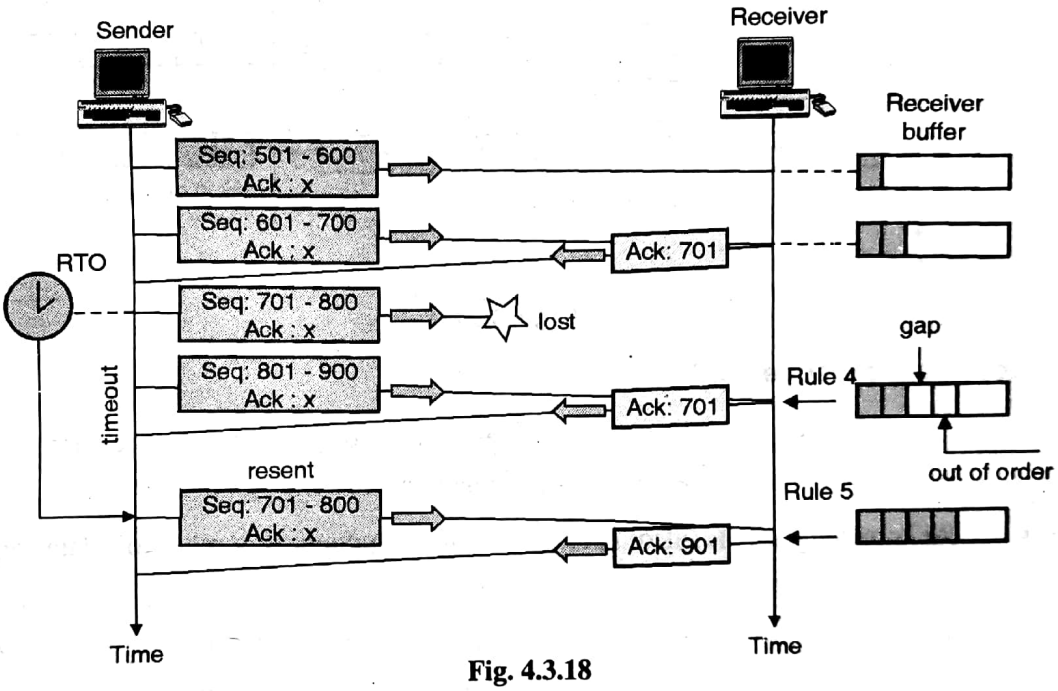


Fig. 4.3.18

(b) Fast retransmission :

- After the lost of segment the receiver sends acknowledgement for particular data transmission.
- If sender gets the 3 acknowledgements then sender retransmit the segment before the timer goes off.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

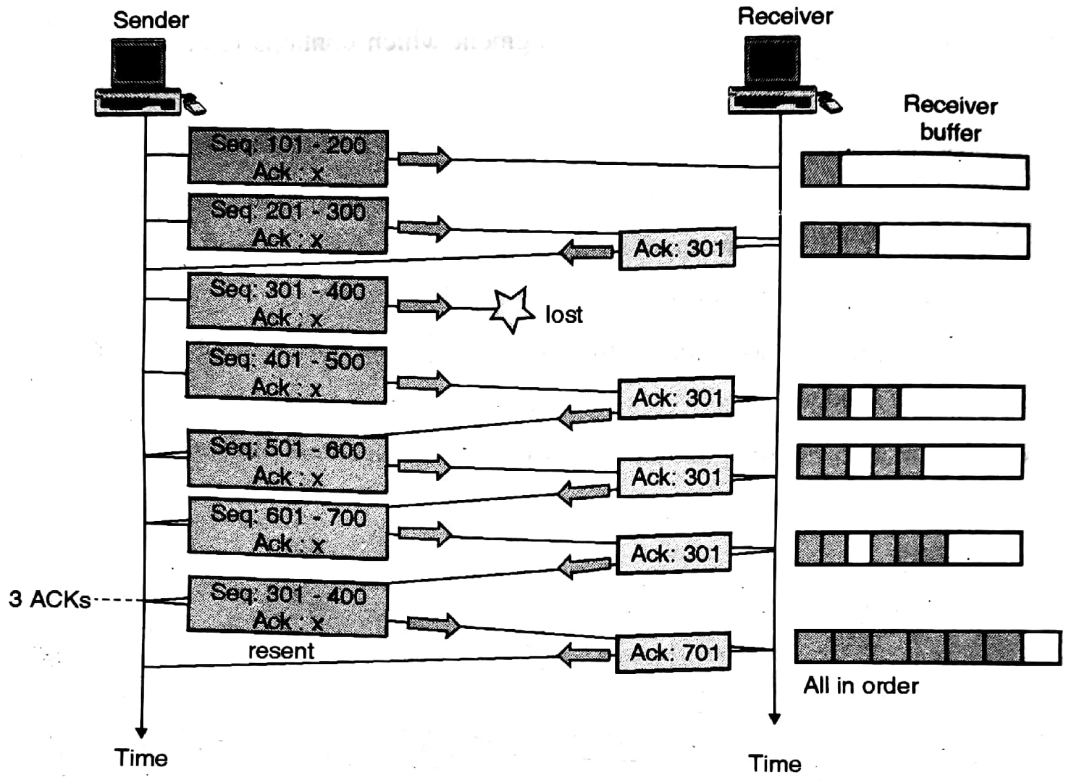


Fig. 4.3.19

(c) Lost Acknowledgement :

- The successful transmission of segments from sender to receiver's side are mentioned with the help of acknowledgements.
- Acknowledgements also specify the next sequence number of data segment expected by receiver.
- If due to some problems in the network sometimes the ack segments does not reaches to the destination it just gets lost in between the path.
- Due to which sender does not get any idea about what is requirement from the receiver's side.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

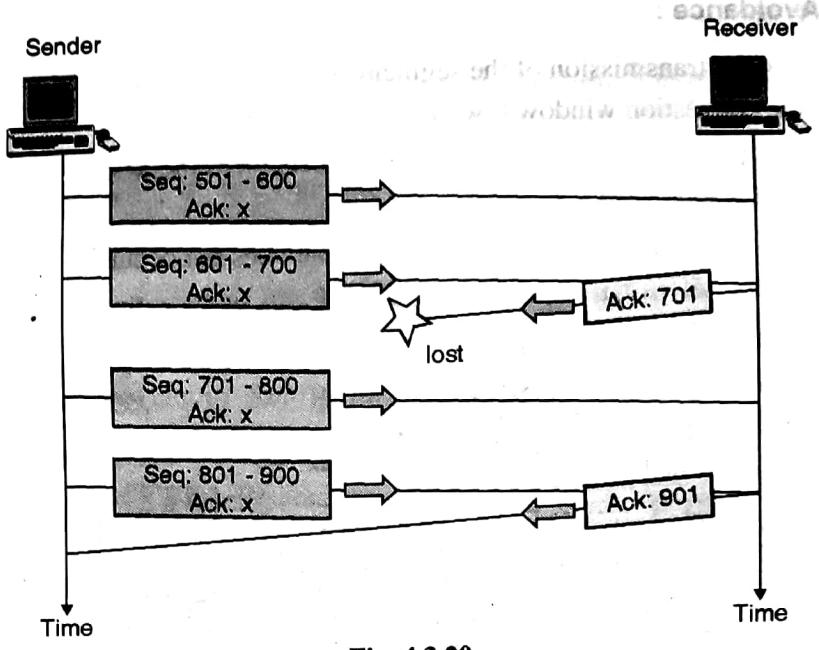


Fig. 4.3.20

(d) Lost acknowledged corrected by resending :

As we have seen above due to some network issues the ack segment does not reaches to the sender of a segments.

Q. Due to which it does not get an idea whether the data is reached to the receiver's side and next which data to be send?

Ans. :

- To avoid all these problems we are able to do the retransmission of segment after a particular time slot called as "timeout concept".
- As shown in the figure the sender sends two segments with the sequence number 501- 600 and other 601 - 700 and starts a timer to get a acknowledgement from receiver.
- The receiver sends an acknowledgement which specifies next expected sequence number as 701 ; but the ack gets lost.

  Sender waits till the end of set timer or else it considered it as lost acknowledgement and sends the same sequence segment to the receiver again.

4.3.18 Congestion Control :

- While transmitting data segments between sender and receiver's side if the speed is not taken in to consideration the flooding of the path takes place.
- The TCP provides important mechanism to avoid the congestion in the network.
- It helps to keep limited number of data segments in the network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Congestion Avoidance :

- While doing the transmission of the segments between the sender and receiver after each segment the congestion window (cwnd) size is increased by one.
- As shown in the Fig. 4.3.21 after sending each segment the ack is send by the receiver and the cwnd is increased.
- The window size is increased until the congestion does not occurs.

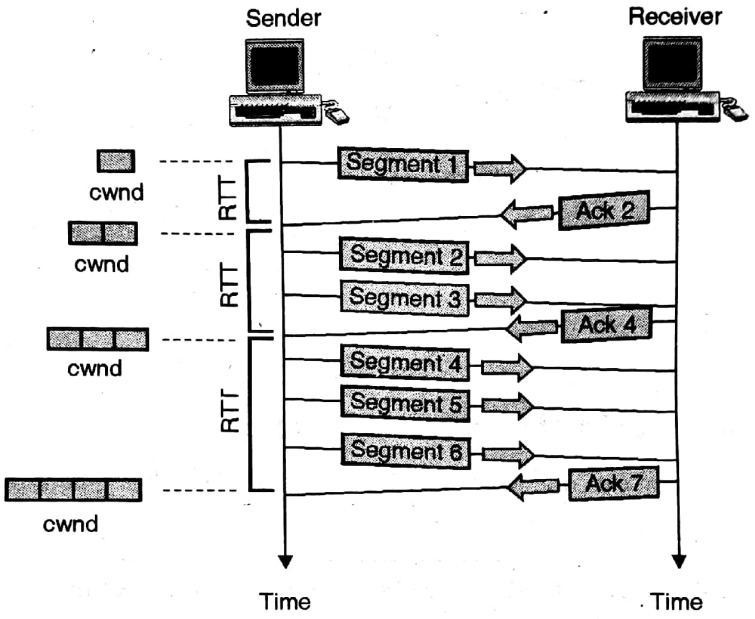


Fig. 4.3.21

Congestion Example :

In the graph :

- x-axis : shows congestion window
- Congestion window size < receivers window size

There are three types :

1. Slow start
2. Adaptive increase
3. Multiplicative decrease

1. Slow start :

- At the start the data transfer rate is slow.
- Then when it reaches to a threshold value 16 the next type starts.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2. Adaptive increase :

- When congestion window reaches to threshold limit it starts adaptive increase.
- Till the time out till the window size reaches to 22.
- After this point the size can not be increased.

3. Multiplicative decrease :

- After this step when the size of congestion window decreases to a particular threshold the data segments are not forwarded over the network.
- When it reaches to size 10 again the three steps are followed as per the pre decided limits.
- The data is shown in Fig. 4.3.22 as per the thresholds and congestion window size.

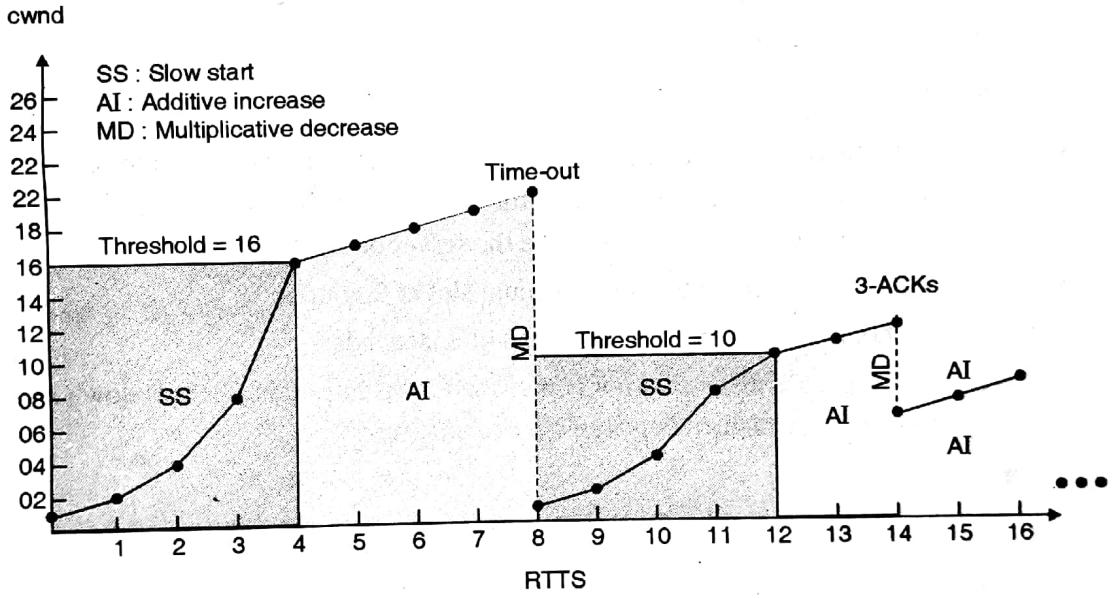


Fig. 4.3.22

4.3.19 TCP Timers :

Q. Explain the timers used in Transmission Control Protocol. MU - April 2013

In TCP there are four major types of timers we consider :

(a) Retransmission :

When sender sends segment it starts a timer to check the details if any error occurs in between the transmission.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(b) Persistence :

- When sending TCP receives window size as zero and waits till it becomes non-zero.
- If acknowledgement sent by receiver which ensure about non zero window size is lost in between than at this situation client waits for the ack for long time.
- It uses probe(special segment) concept is used.
- If after the first probe also response does not comes from the sender side than again the probe is send.

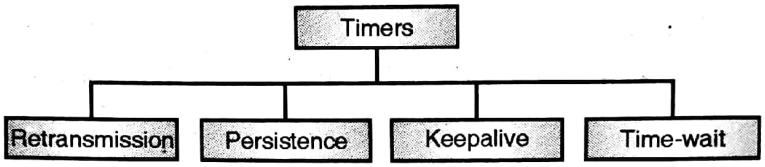


Fig. 4.3.23

(c) Keep alive :

- If the connection in between client and server exists and due to some reason from both of them if any one remains idle for long time other side thinks the connection is still exist where the situation is like the server or client has been crashed.
- The time out is used here with maximum slot of 2 hours.
- After 2 hours it sends probes in the gap of 75seconds.
- If after 10 probes also reply not comes than it assumes that client is down and the connection is terminated between client and server.

(d) Time - wait :

The time wait timer is considered as 2MSL which is used during the connection termination.

4.3.20 TCP Options :

Q. List the multiple byte options supported by TCP. Explain any one with proper example. MU - April 2013

- The TCP header contains around 40 bytes for optional information.
- Options helps to specify the extra information about the destination system.
- There are two types of options;
  1. Single byte:
     - End of option
     - No operations

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2. Multiple Byte:
   - Maximum segment size
   - Window scale factor
   - Timestamp
   - SACK permitted
   - SACK

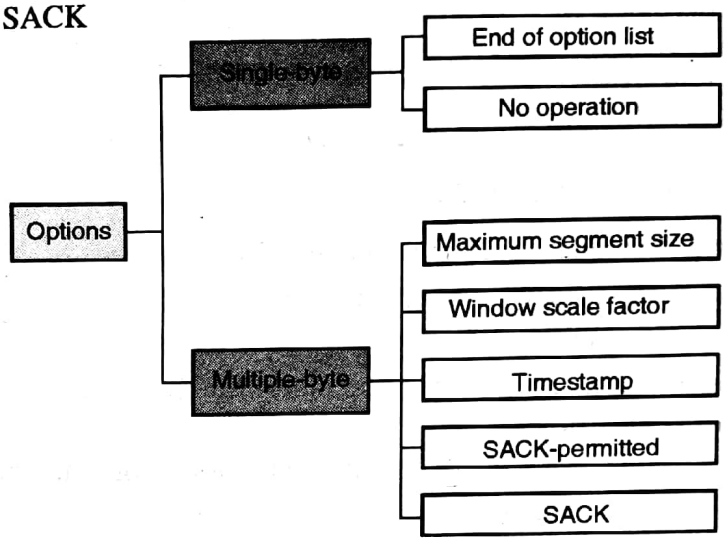
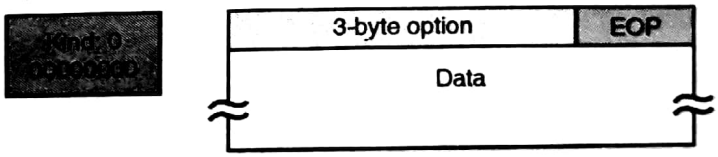


Fig. 4.3.24

(a) End of Option :

- This option able to used only once with all 0's as shown in the Fig. 4.3.25.
- It belongs to kind 0 of single byte options. Which can be also use for padding of data.



a. End of option list b. Used for padding

Fig. 4.3.25

(b) No Operation Option :

- We are able to use it more than once.
- It belongs to kind 1 of single byte options.
- It is useful for aligning the beginning of an various options.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

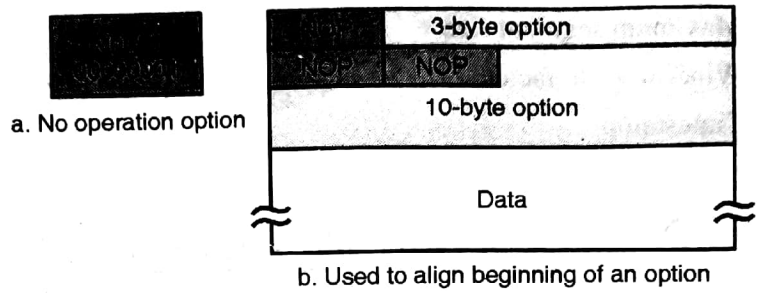


Fig. 4.3.26

(c) Maximum segment size of option :

- As shown in the Fig. 4.3.27 the option is of total 4 bytes.
- 1 byte – specifies the Kind of option with 8 bits.
- 1 byte – specifies length of option
- 2 bytes – specifies the maximum segment size can be considered while transferring the data
- It is considered at the starting of the transmission of data and does not change during the transmission.

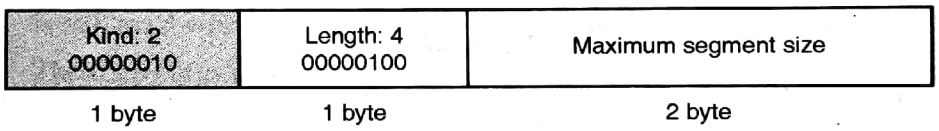


Fig. 4.3.27

(d) Window Scale factor option :

It is also specified at the connection establishment and remains same till the termination.

It contains;

- 1 byte – for kind 3 option of multi byte
- 1 byte – to mention length 3
- 1 byte – to specify the scale factor.

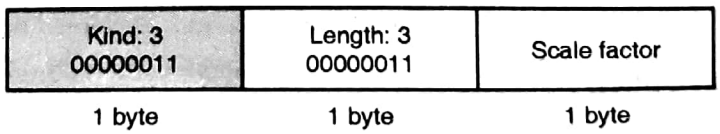


Fig. 4.3.28

(e) Time Stamp option :

Time stamp option specifies the following field like;

- Kind 8 of multiple byte option

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Total length 10 bytes
- It helps to calculate RTT i.e. Round Trip Time

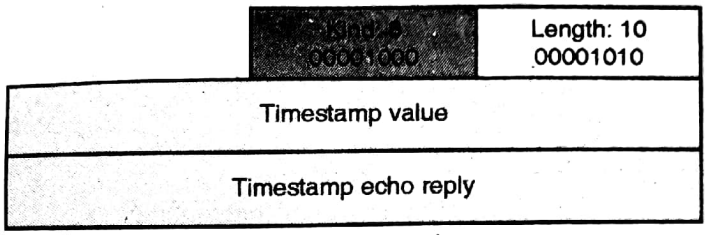


Fig. 4.3.29

4.3.21 TCP Package :

- TCP package is as shown in the Fig. 4.3.30.
- TCP package describes tables called transmission control blocks, a set of timers, and three software modules.

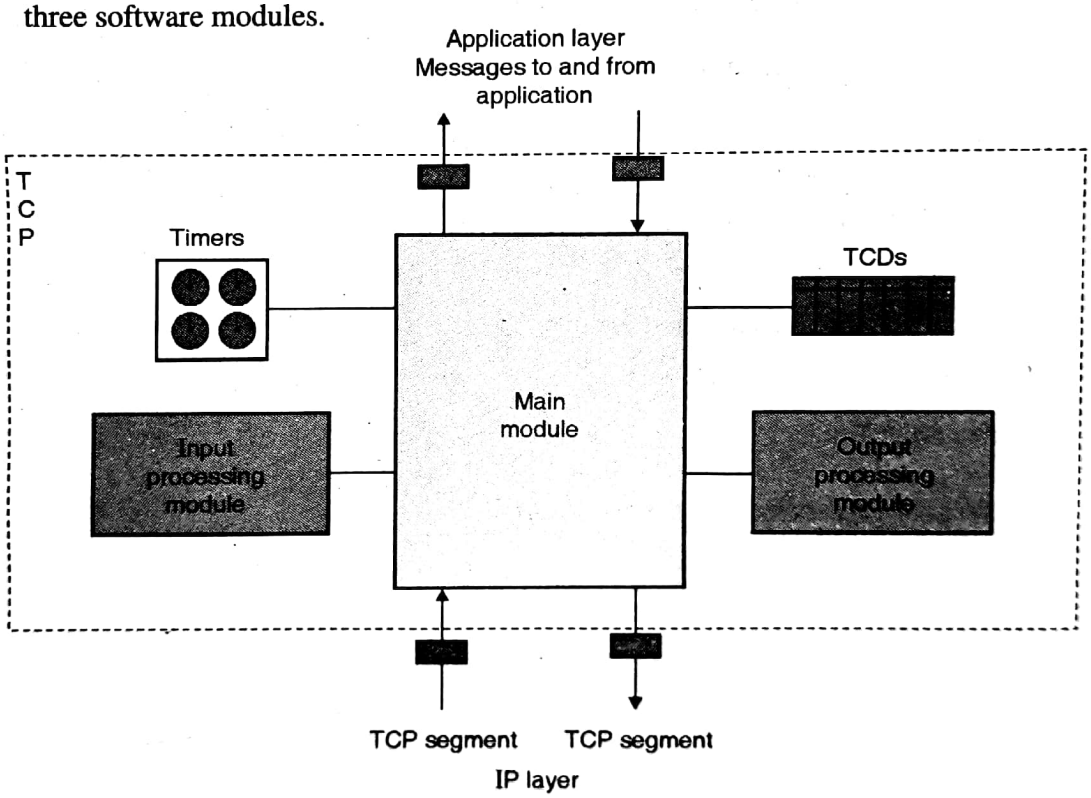


Fig. 4.3.30 : TCP package

(a) Transmission Control Block :

It specifies fields like:

- **State :** It specifies the status of the process
- **Process :** It mentioned which process is mentioned in the particular entry

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Pointer :** It helps to point the buffer in which the data entry is done related with the particular process.

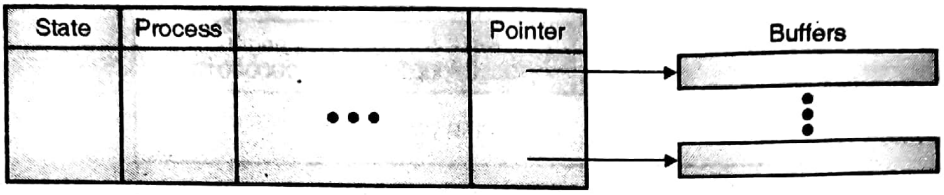


Fig. 4.3.31 : Transmission control block

Review Questions

Q. 1 Write short node on UDP.

Q. 2 Explain use of buffer in TCP.

Q. 3 Explain various TCP connections in detail.

Q. 4 What is silly window syndrome in TCP.

Q. 5 Explain UDP packet in detail.

Q. 6 Explain TCP packet in detail.

Q. 7 Explain TCP State Transition diagram in detail.

Q. 8 TCP Package in detail.

Q. 9 What is simultaneous close and open in TCP.

Q. 10 Difference between TCP and UDP.

Q. 11 What is Sync Flooding attack in TCP.

4.4 University Questions and Answers

April 2013

Q. 1 Explain the timers used in Transmission Control Protocol. **(Sections 4.3.19) (5 Marks)**

Q. 2 List the multiple byte options supported by TCP. Explain any one with proper example. **(Section 4.3.20)** **(5 Marks)**

Q. 3 A TCP connection is in ESTABLISHED. The following events occur one after another.

(a) FIN segment is received

(b) The application sends a "close" message.

(Section 4.3.10) **(5 Marks)**

www.MumbaiBScITStudy.Com

CHAPTER 5

Application Layer

Syllabus

- SCTP
- DHCP
- Domain Name System (DNS)

5.1 Stream Control Transmission Protocol (SCTP)

5.1.1 Position in TCP / IP Model :

- SCTP (Stream Control Transmission Protocol) belongs to the transport layer protocol and useful to connect client process to server process.
- Since we have already seen UDP having some issues hence we have seen TCP.
- Now SCTP is one which considers merits of UDP and TCP.
- It is reliable protocol.
- It uses cookies to give details about the data segment like sequence number, port number, size of segment etc.
- Like TCP, SCTP establishes association between client process and server process.

Mumbai B.Sc.IT Study

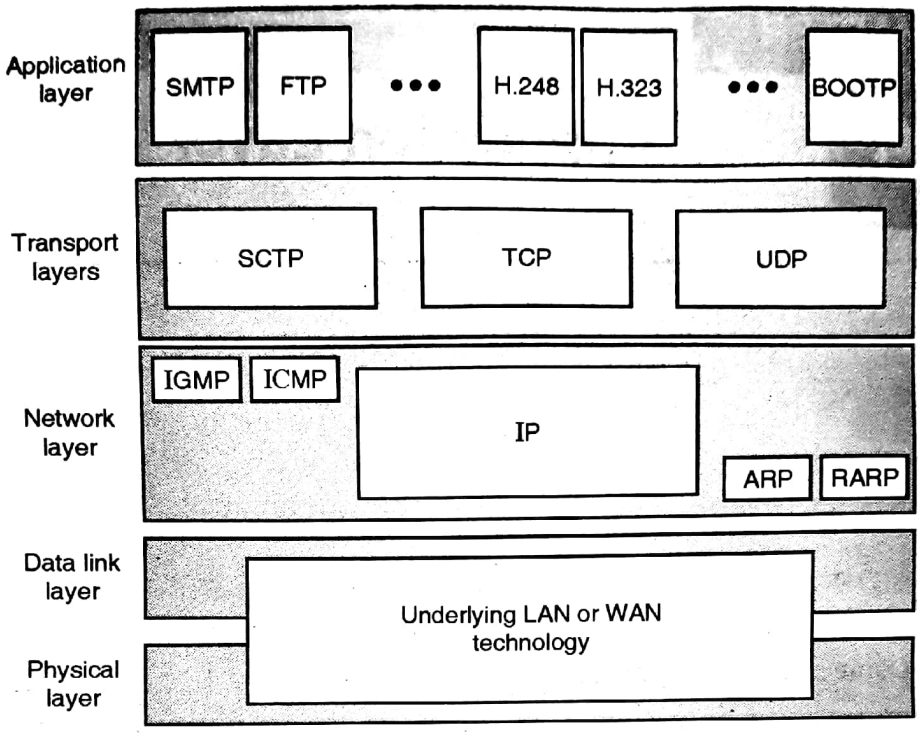


Fig. 5.1.1

5.1.2 SCTP Application :

Some SCTP application protocols along with the port numbers are listed below :

- SIP – 5060

  Useful for IP telephony.

- IUA – 9990

  Helps for ISDN over IP

- H.248 – 2945

  Provides media gateway control.

5.1.3 Multiple Stream Concept :

By using TCP we have send only one stream at a time between sender and receiver but now with the help of SCTP we are able to transfer multiple streams between sender and receiver.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

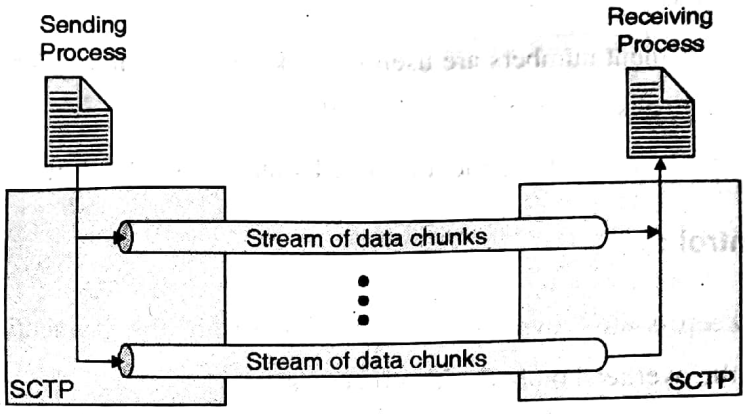


Fig. 5.1.2

Advantage :

- Due to the multiple stream transmission at the same time the data transfer can be done with multiple processes using IP address of the sending and receiving process ends.
- In SCTP we consider a group of data called as "data chunks" are transferred via a stream among the sender and receiver.
- Each stream contains number of data chunks and such number of streams can be transferred.

5.1.4 SCTP Features :

Q. Explain the features of Stream Control Transmission Protocol **MU – April 2013**

Transmission Sequence Number (TSN)

The unique number given to transmitted data chunks known as "TSN" i.e. Transmission Sequence Number. It informs about the association in SCTP.

Stream Identifier (SI)

Since SCTP allows to transfer the number of data streams over the connection to identify individual stream differently "Stream Identifier" is used. Unique stream is given by SI.

Stream Sequence Number (SSN)

- To identify data chunks which are belongs to the same data stream.
- To mention the data chunks of one stream SCTP uses "SSN" i.e. Stream Sequence Number Packets.
- It gives unique number to the data chunk belongs to the same stream.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Acknowledgment Number

- The acknowledgement numbers are useful to acknowledge only number of data chunks. It does not help to acknowledge control chunks.
- The control chunk acknowledgement is done by another control chunks.

5.1.5 Flow Control :

It helps to keep control over the data flowing within the connection of sender and receiver. To avoid the overhead on both side processes.

5.1.6 Error Control :

It helps for error control also as we get in TCP.

5.1.7 Congestion Control :

It helps to avoid congestion over the network and try to keep connection congestion-free.

5.1.8 TCP VS SCTP Packet :

TCP Segment

- It has been divided into two parts "Header and options" and "data bytes".
- We have seen TCP sends data in the form of segments containing various fields.

SCTP packet

- The SCTP has three main parts; "Header", "Control" and "data bytes".
- Along with this it contains fields like;
  1. Source port address, destination port address
  2. Verification tag
  3. Checksum
  4. Control chunks
  5. Data chunks:
- Data chunks inform about three identifiers: TSN, SI, and SSN.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

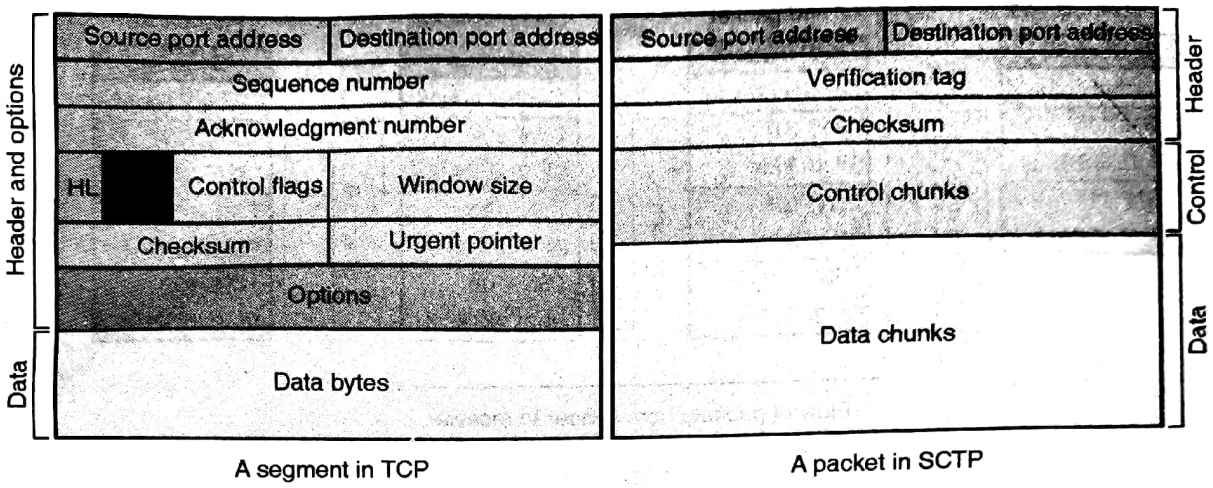


Fig. 5.1.3 : Comparison of TCP and SCTP packets

5.1.9 Packet, Data Chunks, and Streams :

As shown in the Fig. 5.1.4 there are :

- 4 packets, each having Header, control chunk and data chunk.
- Data chunk maintains information about various chunks of data belonging to the individual stream.

As shown below:

- Fields of First packet
- Header
- Control chunks
- Data chunks

It contains TSN , SI and SSN of individual data chunk.

Here,

First packet contains three data chunks and there description is as follows:

TSN : 101 SI : 0 SSN : 0

TSN : 102 SI : 0 SSN :1

TSN : 102 SI : 0 SSN :2

It transfers streams over the connection for sharing of data.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

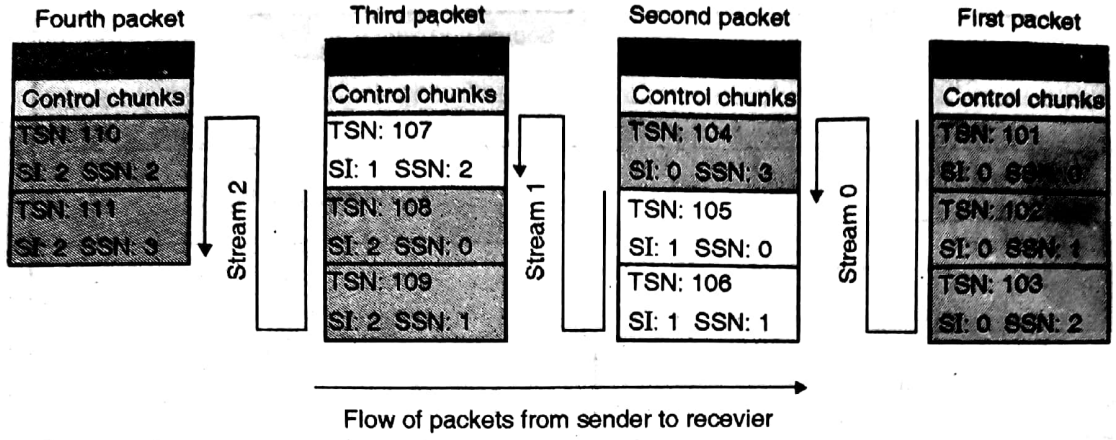


Fig. 5.1.4

5.1.10 SCTP Packet Format :

TCP send data in segments whereas SCTP sends data in packet format.

It has fields like:

- Header : 12 bytes
- Control chunk and Data chunk : variable length.
- In the SCTP packets control chunk specifies first than data chunks.

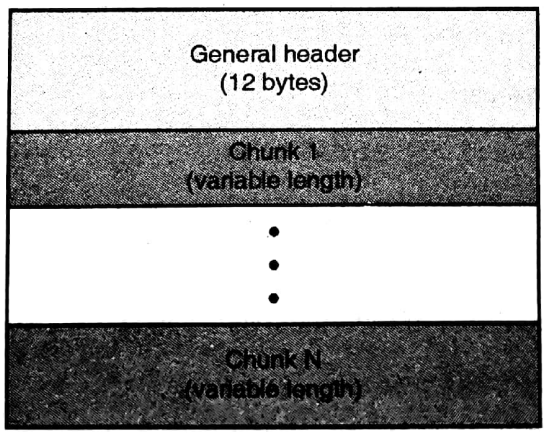


Fig. 5.1.5

(a) General header

The SCTP header has following fields :

- **Source Port address : 16 bits (2bytes)**
  It indicates the port number of application executing on source process.
- **Destination Port address : 16 bits (2bytes)**
  It indicates the port number of application executing on destination process.
  Verification Tag : 32 bits (4 bytes)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Checksum : 32 bits (4 bytes)**

  It helps to find out error occurred while transmission of data stream over the connection.

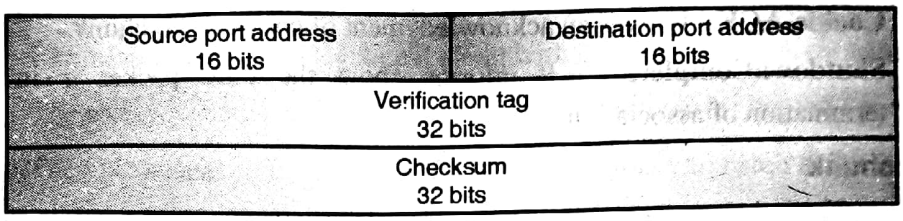


Fig. 5.1.6

(b) Common layout of chunk :

The SCTP transfers data streams over the network with number of data chunks.

Each chunks has following fields:

- Type : 8
- Flag : 8
- Length : 16
- Chunk information: Multiple of 4 bytes

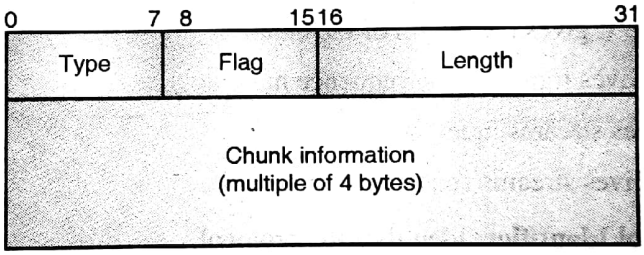


Fig. 5.1.7

5.1.11 Chunks :

- Chunks need to be terminating within a boundary of 32 bits i.e 4 bytes.
- "Cookies" gives data which is important for server for server for sending reply
- Some chunks along with the descriptions are listed below:
  - **User** - describes a user data
  - **INIT** - tells about starting an association between sender and receiver
  - **INITACK** - informs about acknowledgment of INIT chunks.
  - **SACK** - informs only about selective chunks.
  - **Abort** - It helps to abort an association between client process and server process.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Shutdown** - It helps to terminate an association between client and server
- **Error** - It inform about the errors without shutingdown the connection.
- **Cookie Echo** - It tell that third packet is ready for association.
- **Cookie-ACK** - It gives an acknowledgment of cookie echo chunk
- **ShutdownComplete** - It informs about the third packet is in ready for termination of association

(a) Data chunk

- Data chunks at a time carries data of one message and can be consider parts of same message but not of other message.
- Data chunks carries at least one byte of data.
- Data chunks are the only one which are acknowledge.
- It contains TSN i.e. Transmission Sequence number gives number to be given to the data chunks

Fields of data chunks are listed down

- **Type** : various type codes are considered for data chunks
- **Reserved**: some bits are reserved for the use.
- **Length**: It gives the length of the chunk
- **TSN**: Gives transmission sequence number
- **SI**: Gives streams index number.
- **SSN**: Gives streams sequence number
- **Protocol Identifier**: Identifies the protocol
- **User data**: Describes the data

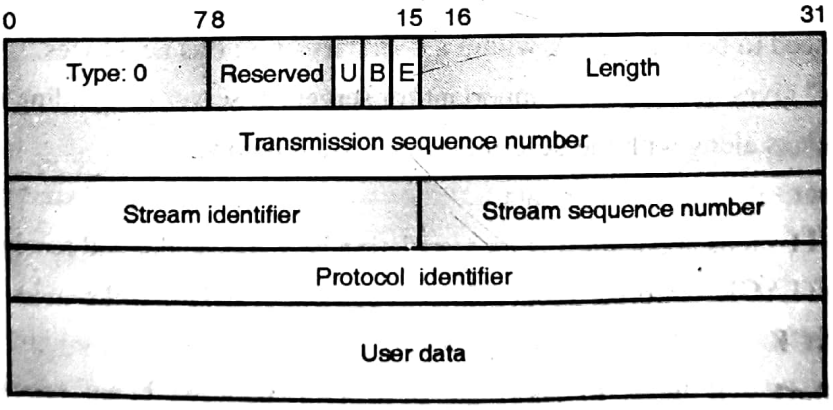


Fig. 5.1.8

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.1.12 Connection Establishment :

(a) Four way hand shaking :

When client wants to establish connection between client process and serve process :

- Client process sends INIT signal along with the TSN and receiver window(rwnd).
- The receiver sends INITACK as an acknowledgement for the INIT to the sender.
- Then the sender sends Cookie-ACK to tell that ready to listen next signal
- Cookie-ack is send as an acknowledgement to the client from the server.

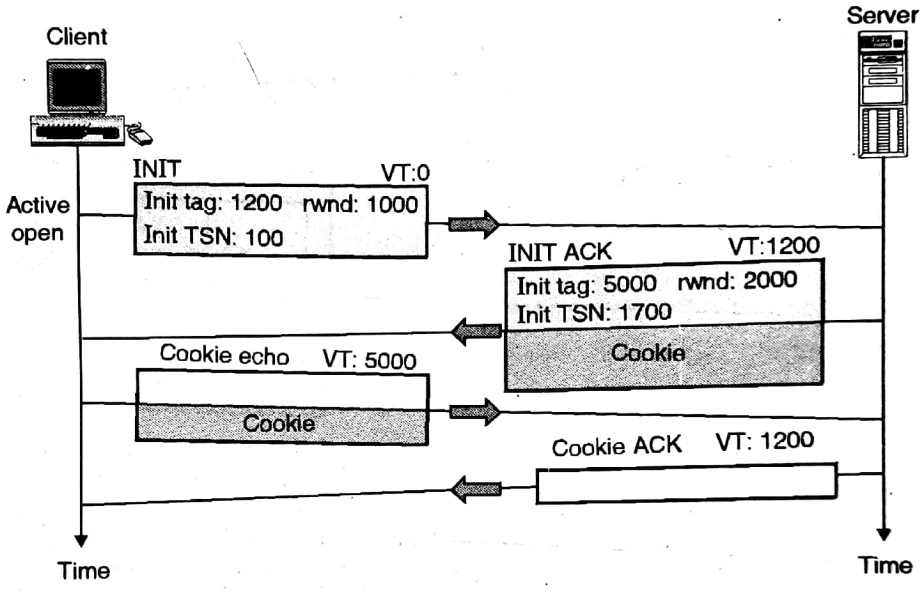


Fig. 5.1.9

(b) Simple data transfer :

- After establishing connection between client and server
- Client sends chunk of data along with the TSN of individual data chunk
- Through sack Signal the selective acknowledgements are send from server to client along with some data chunks.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

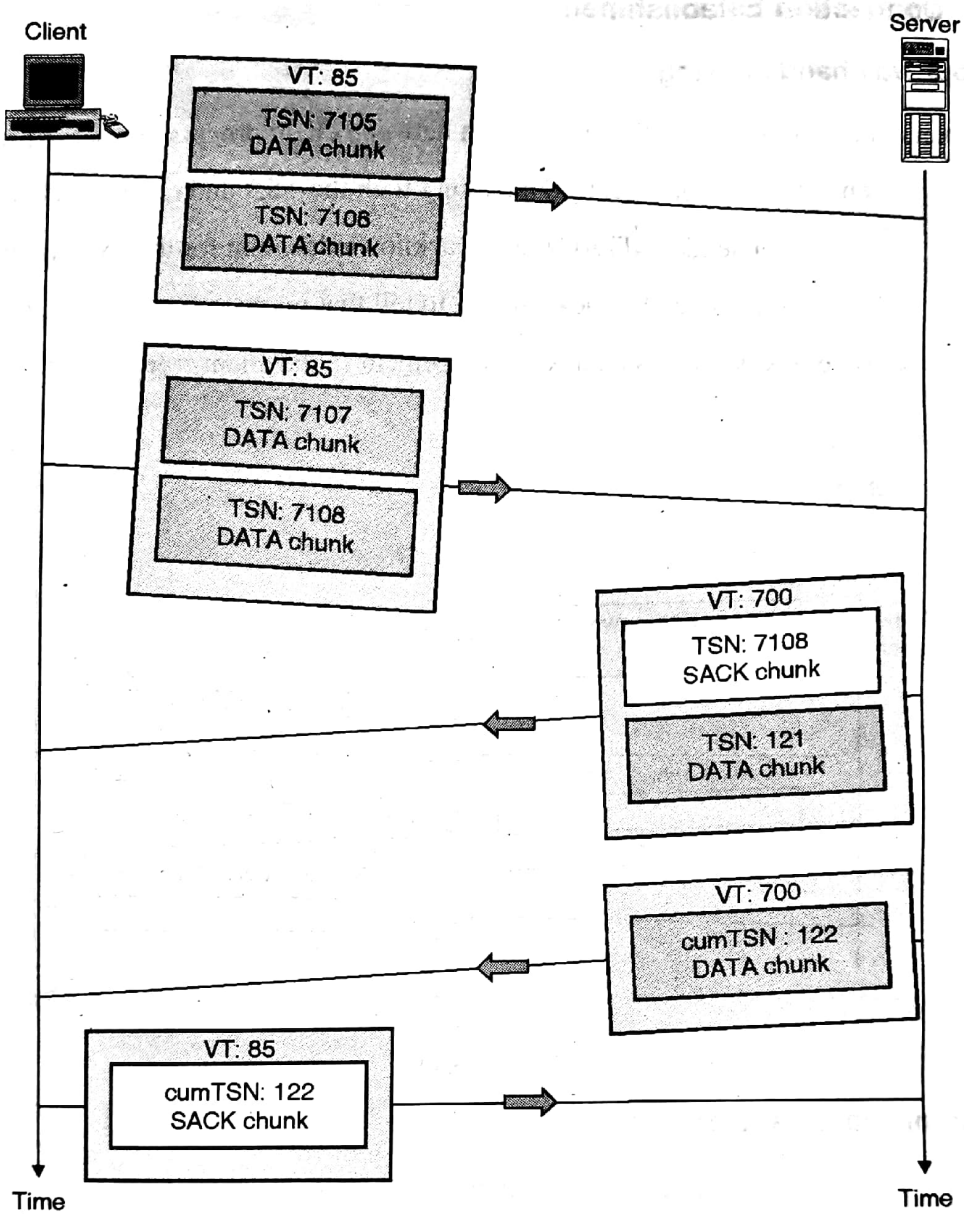


Fig. 5.1.10

(c) Association Termination

- To active close the connection between client and server the client first sends a shutdown signal to server.
- Then waits for shutdown-ACK from server.
- Whenever acknowledgement of shutdown signal send by server to client the ShutdownComplet signal send by client to server.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

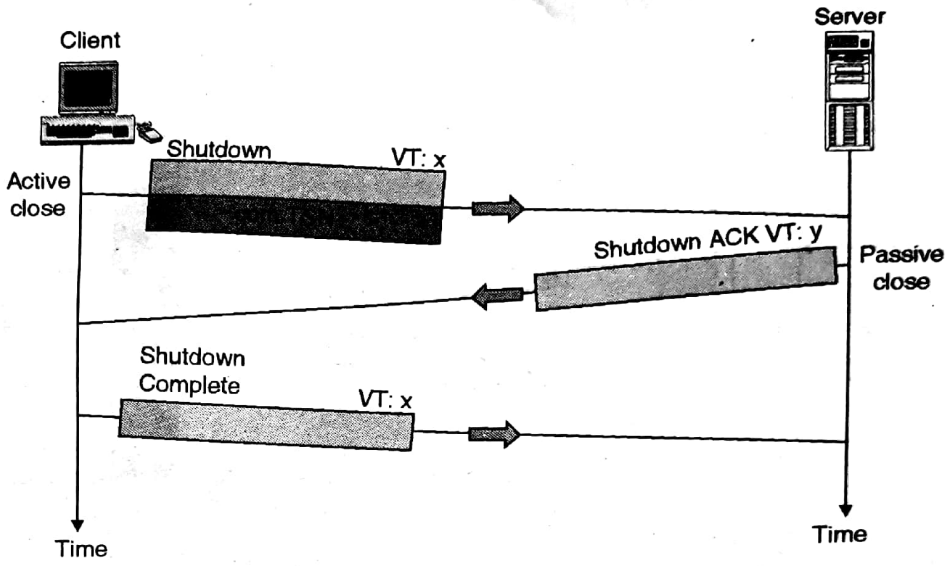


Fig. 5.1.11

(d) Association Abortion

If there is any problem occur during the transmission client sends an abort signal to the server for terminating connection.

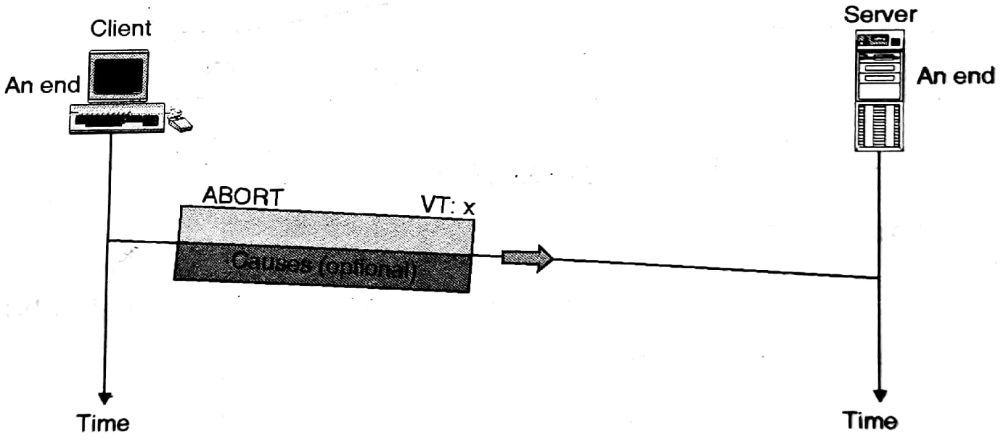


Fig. 5.1.12

(e) Simultaneous Open

- Both the client as well as server sends an INIT signal for the connection establishment.
- After getting INIT-ACK the cookie-echo send to respective receiver.
- Then the receiver sends cookie-ack and the connection is established between client ad server.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

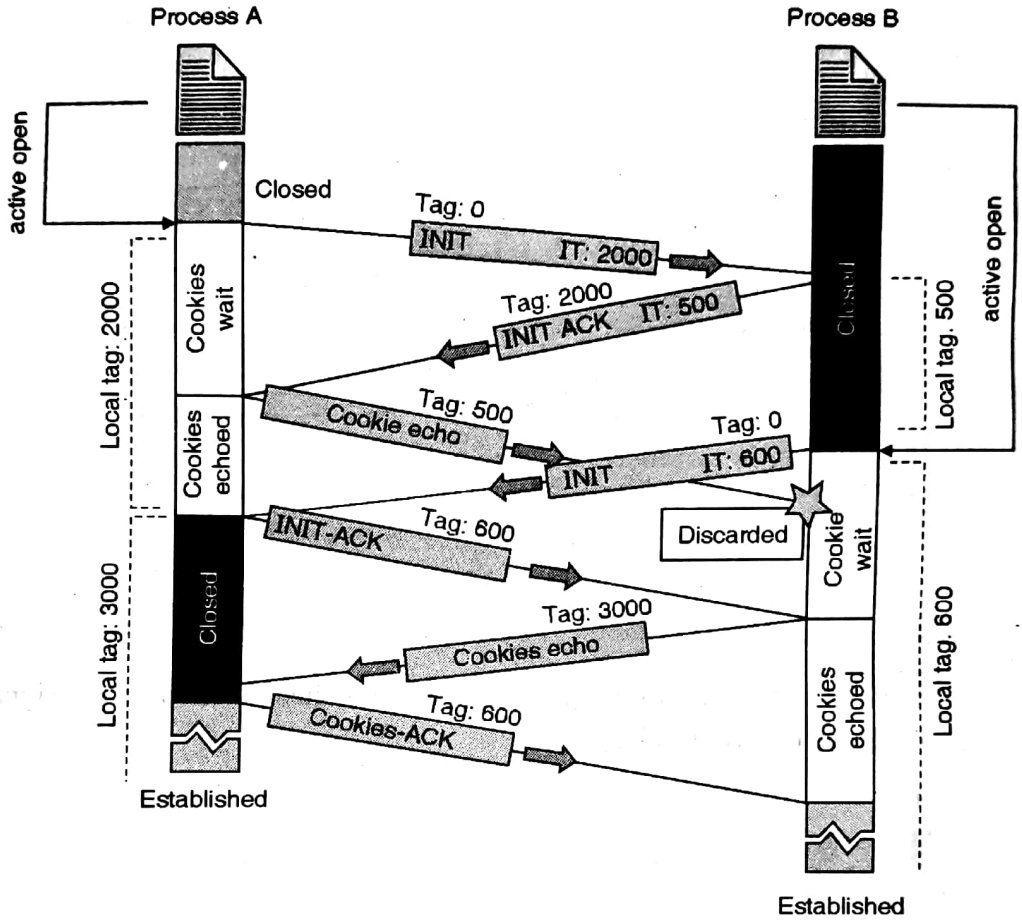


Fig. 5.1.13

(f) Simultaneous Close

1. As we can see in the Fig. 5.1.14 the connection has been established between client process and server process.
2. When both the ends decide about closing the connection. Simultaneously both of them sends shutdown packet to each other.
3. Then shutdown-ACK Sent by both the parties to each other.
4. After receiving shutdown-ACK bothe the ends sends shutdown-complete and the connection between the sender and receiver is closed.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

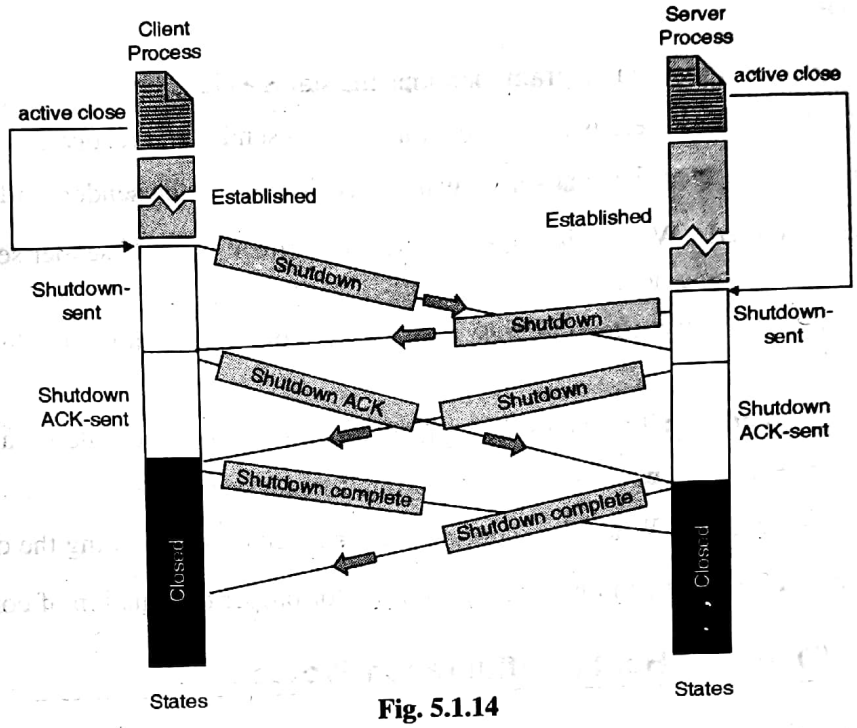


Fig. 5.1.14

5.1.13 State Transition Diagram :

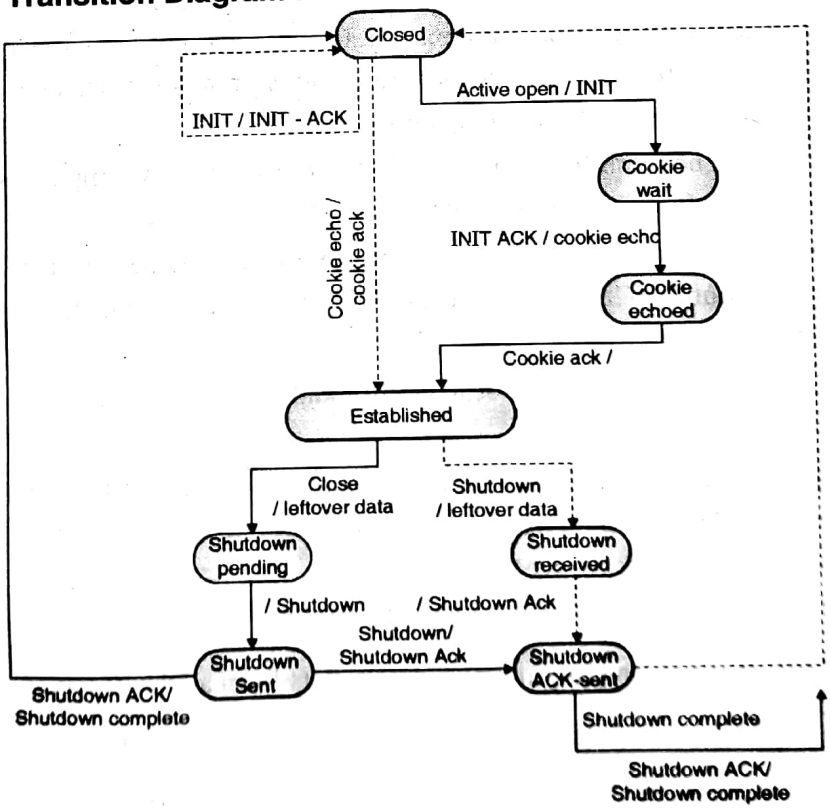


Fig. 5.1.15

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sate for SCTP :

The SCTP state transition diagram mentions the states as listed below:

(a) **Closed :** It specifies there is no connection between sender and receiver.

(b) **Cookie- wait :** It specifies that server wait for cookies from the sender's side.

(c) **Cookies - Echoed :** When client get an acknowledgment of INIT sender sends response as waiting for cookie-ack.

(d) **Established :** Finally after the four way sharing the connection establishes between client and server.

(e) **Shutdown- pending :** The data sending is going on still the close state is called.

(f) **Shutdown- Sent :** In this state client is waiting for shutdown-ack.

(g) **Shutdown-received :** When the shutdown-ack is received still sending the data.

(h) **Shutdown-ACK-sent :** In this sate it is waiting for proper termination of connection.

5.2 DHCP (Dynamic Host Configuration Protocol)

5.2.1 Introduction :

- DHCP (Dynamic Host Configuration Protocol) is a protocol used for automatic assignment of IP (Internet Protocol) configurations on a computer network and can be manage centrally by network administrators.
- In the computer network for communicating with each other; computer system requires the systems must have unique IP address.
- In the present scenario computers are frequently moved and new systems get added to a network. Without DHCP, the IP address must be entered manually at each computer system.
- DHCP helps network administrator to control and distribute IP addresses from a central point.
- The purpose of DHCP is to provide the dynamic allocation of IP client configurations for a specific time period (called a lease period) which reduces burden from administer to handle whole network manually.
- Client-Server model is useful for working of DHCP.

  Client : A host requesting initialization parameters from a DHCP server.

  Server : The host providing initialization parameters through DHCP
- DHCP server hosts all located network addresses and deliver required configuration parameters to dynamically configured hosts.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.2.2 DHCP Packet Format :

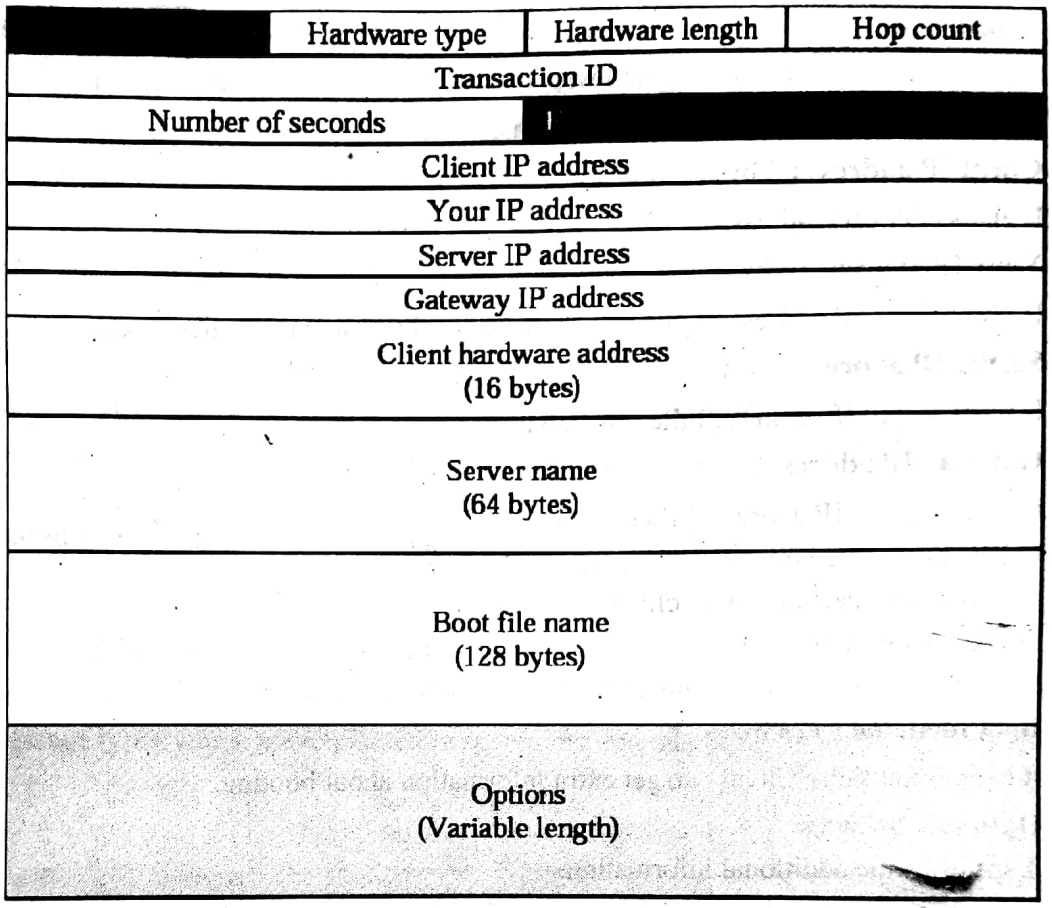


Fig. 5.2.1 : DHCP packet Format

The fields of DHCP packages are as follows:

- **Operation code :** 8 bits

  Defines two types; "request" by 1 and "reply" by 2
- **Hardware type :** 8 bits

  It defines the type of physical network like Ethernet value is 1.
- **Hardware Length:** 8bits

  It defines the length of physical address in bytes like Ethernet value is 6.
- **Hop count :** 8 bits

  The number of hops the packet travel while travelling from source to destination.
- **Transaction ID:** 4 bytes

  It is given by client to each packet by which it can match to the reply send from the server.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Number of seconds:** 16 bits
  The time passed from when the client boot in.
- **Flags:** 16 bits
  from the flag first bit is mentioned with 0 or 1 and other 15 bits are zero bits.
  0 means "Unicast" and 1 means "broadcast"
- **Client IP address :** 4 byte
  It gives client IP address.
- **Your IP address :** 4 byte
  It gives client IP address. It is filled by server in the reply at the clients request.
- **Server IP address :** 4 byte
  It gives server IP address. Filled by server.
- **Gateway IP address :** 4 byte
  It gives routers IP address. Filled by server.
- **Client hard ware address :** 16 byte
  It gives physical address of client.
- **Server Name :** 64 bytes
  It is optional field. Gives domain name of server.
- **Boot filename :** 128 bytes
  It is optional field, Client can get extra information about booting.
- **Options :** 64 bytes
  It specifies the additional information.
  It specifies three fields:
  1 byte for tag , 1 byte length and other is variable for length field.

5.2.3 DHCP Address Allocation :

- DHCP is used to provide static or dynamic address allocation which can be done at manual or automatic
- **Static Address Allocation :** A DHCP server has a static database which can be bounded to the physical addresses to IP addresses.
  Dynamic Address Allocation : DHCP server will provide the temporary dynamic IP addresses for some limited time frame. Such addresses are temporary addresses used from free pool of IP addresses. After some time DHCP server either issues new IP address or again renew same address for some more time.
- **Configurations**
  - Automatic – Dynamic IP addresses are created automatically
  - Manual – Static IP addresses are assigned by DHCP server manually.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.2.4 Working :

- Client broadcasts a request for the address information from systems while starting with TCP connection.
- DHCP server receives a request from client then it assigns a new address for a specific time interval to a system called as **Lease Time** meaning no wasted numbers.
- DHCP server sends these dynamic addresses to the client together with the other required configuration information.
- To set up its configuration this information is acknowledged by the client system.
- The DHCP server will not restructure the address during the lease period and will attempt to return the same address every time the client requests an address.
- The client may extend its lease by requesting for it and may send a message to the server before the lease expires. Explaining that it no longer needs the address so it can be released and assigned to another client on the network.

5.2.5 DHCP Message Passing :

The DHCP connection states are as shown below :

The message passing between client and server takes place by using the following various message types which are explained in state transition diagram

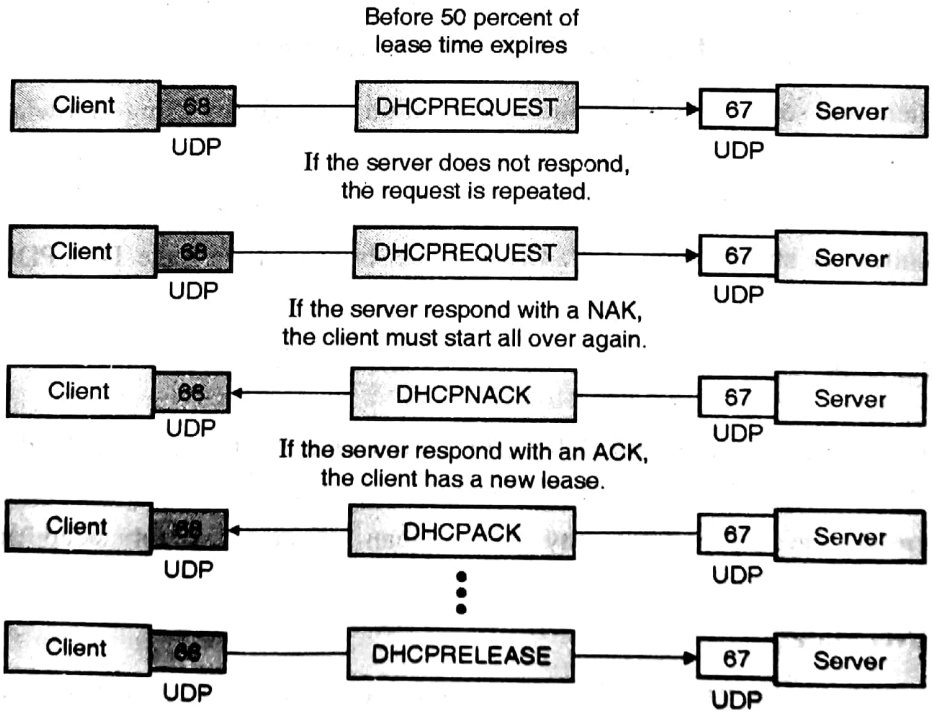


Fig.. 5.2.2 : DHCP Message Passing

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.2.6 DHCP Transition Diagram :

Q. Explain the DHCP client transition diagram. **MU April 2013**

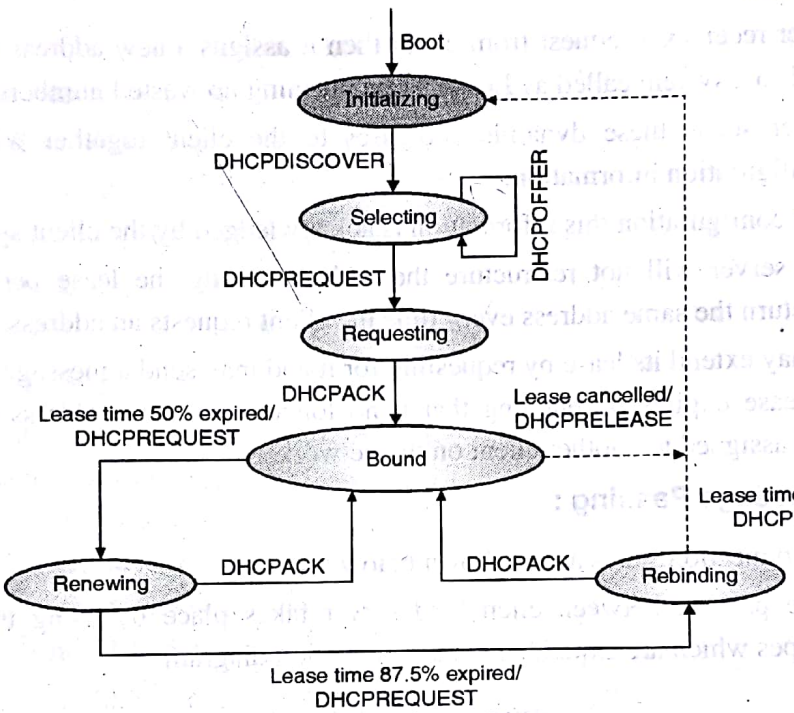


Fig. 5.2.3: DHCP Transition Diagram

The client and server sends dynamic configuration messages by using following states:

INIT State

It is called as initialization state. Client sends broadcast message DHCPDISCOVER using port 67.

SELECTING State

The server than response with DHCPOFFER message and blocks own IP address to be unavailable for other users.

If there is no reply from any server than client goes for sleep and sends DHCPDISCOVER again.

REQUESTING State

Client sends DHCP REQUEST message to the selected server and gets connected with the server using IP address.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Bound State

Client uses IP address of server until the lease time does not become half. If it goes below 50% then again client sends DHCPDISCOVER to renew the connection.

RENEWING State

When client gets DHCACK (acknowledgement) back from server the connection get renewed. If client does not get the DHCACK then It goes to rebinding state.

REBINDING State

If client gets DHCPACK then it goes to the rebind state and connection is established again. Else the client broadcast the DHCPDISCOVER to search new server.

5.2.7 Advantages of DHCP over Manual Configuration Methods :

- The manual configuration of DHCP may require the careful input of a unique IP address, subnet mask, default router address and a Domain Name Server address.
- Computer network is a growing web where it is really difficult for a system administrator to manually add all the IP and the configurations to an individual system where many systems are getting added in the network at every second.
- For a network administrator this process can be lengthy, monotonous and error prone.
- DHCP offers flexibility and ease-of-use.
- From a "set" of existing addresses DHCP server automatically assigned dynamic configuration to each client for a specific time period .
- When a client has finished with the operations, it is released for another computer tc use.

5.2.8 Mobile Computing :

- DHCP is advantageous to provide dynamic addressing in environments where users frequently change locations.
- Mobile users simply plug-in their systems to the network and receive their required configuration dynamically.
- The configuration will be supplied by the network's server when moving to a different network using a DHCP server.
- Manual reconfiguration is not required.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.2.9 DHCP Servers Set-up and Administer :

- DHCP servers manages TCP/IP client configurations like IP address, gateway address and DNS address.
- DHCP servers are easy to setup and are easy to manage.
- Client addresses are assigned dynamically.

5.2.10 Limitations :

- There are some machines on network having fixed addresses for example servers and routers.
- The DHCP server should be capable of assigning some pre allocated addresses to these specific machines.
- Users should be prevented from reconfiguring their own IP addresses to avoid conflicts between automatically configured addresses and manual address.
- We are able to upgrade the system which is having older operating systems because older operating systems do not support DHCP.
- If up gradation is not possible then systems may support the older BOOTP protocol.

5.3 The Domain Name System

- The Internet users are not able to remember the IP addresses of all the web sites that users wanted to visit .
- The *Domain Name System* acts as a bridge between domain names and IP addresses of devices connected in the Internet.
  - A *domain name* (a part of the URL) is a unique alphanumeric name such as gmail.com
  - Here the top level domain name is "com"
  - Secondary level domain name is "gmail".
- A huge amount of data related to various sites is divided among the number of systems to avoid the burden on single system.
- DNS uses services of UDP or TCP on the well-known port 53.
- The working mechanism of DNS is also Client-Server Model.

5.3.1 Name Space :

To avoid the risk of remembering IP addresses now users need to remember the unique names assigned to machines which maps each others.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

There are two types :

(a) Flat name space - Where the names are directly assigned to an address. It is just a sequence of characters.

(b) Hirerarchical name space - In this kind of name space the names are organized as per the hierarchies in the organization.

For example; First part defines Mumbai University i.e. Nature of organization.

Second part defines Engineering College i.e. Part from organization

Thired part defines ABC college i.e. Name of college.

Fourth part defines IT department i.e. Name of department etc.

5.3.2 Domain Name Space :

- The domain name space is defined using the inverted tree structure starts from the root
- **Lable :** Each node in the tree has name called as label. Each node has an unique name to avoid an ambiguities. The lables are used as key in domain name searching.
- **Domain Name :** Each node has a unique domain name.the domain names are read from bottom to root node.Root node is having null name string.
- **For example;** As shown in the Fig. 5.3.1 the lables and domain names are mentioned from bottom node to the root node.

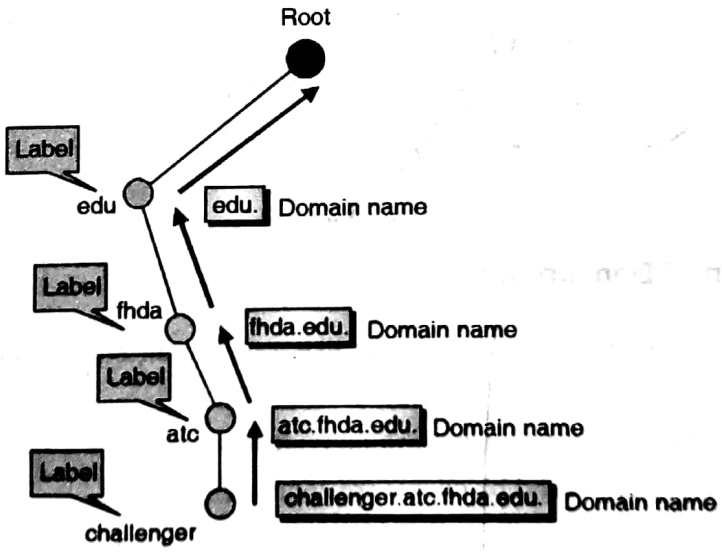


Fig. 5.3.1

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Types of Domain Name :

Q. Define and give example of the following :

(i) Fully qualified domain name

(ii) Partially qualified domain name MU April 2013

(a) Fully Qualified Domain Name :

If the lables are terminated with the root node i.e. Null string then it is known as Fully Qualified Domain Name (FQDN).

For example; as shown in the Fig. 5.3.1FQDN is "challenger.atc.fhda.edu."

(b) Partially Qualified Domain Name :

If the labels are not terminated with the root node i.e. Null string then it is known as Partially Qualified Domain Name (PQDN).

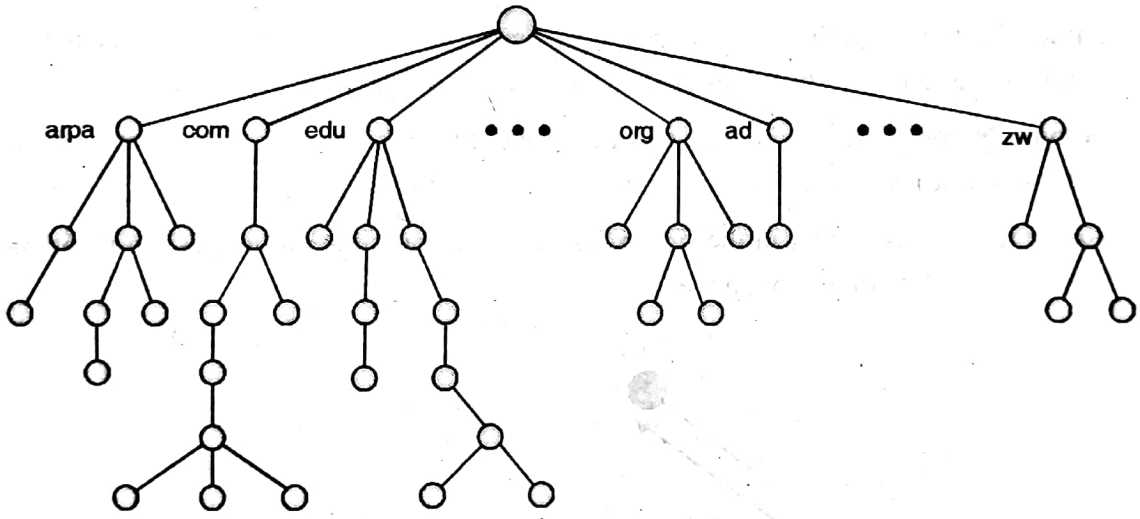


Fig. 5.3.2

5.3.3 Distribution of Domain Names :

- Many servers are connected to root server like arpa server, edu server, com server, us server etc.
- Then further many users are connected to individual servers;
  1. To edu server ; fhda and bk clients are connected
  2. To com server ; mcgraw and Irwin clients are connected
- The root node is classified into various domain servers and further the individual domain server are divided into sub-domain servers.
- There is hierarchies of domain server as it is in the name space.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

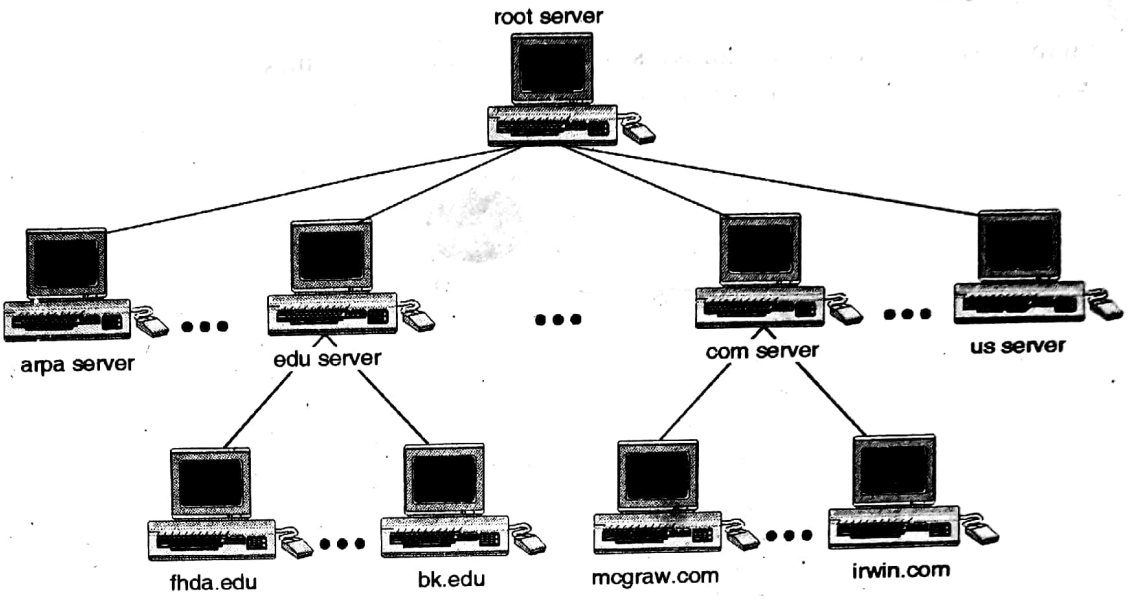


Fig. 5.3.3

5.3.4 Domains :

- IP address and domain name allocation requires central administration to avoid ambiguities.
- This allocation process was previously administered by U.S. government contract (NSI)
- In 1998, technical coordination assigned to ICANN (Internet Corporation for Assigned Names and Numbers).

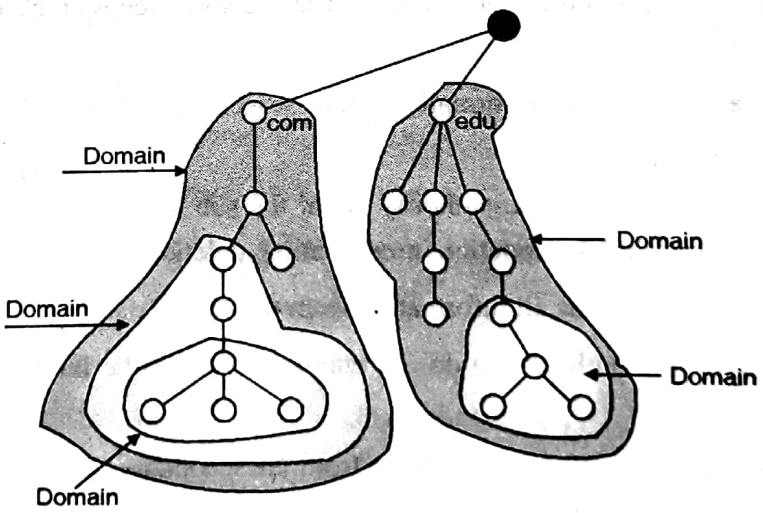


Fig. 5.3.4

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(a) Inverse Domain :

In the inverse domain the address is written from index to names.
For example : 121.45.34.132.in-addr.arpa

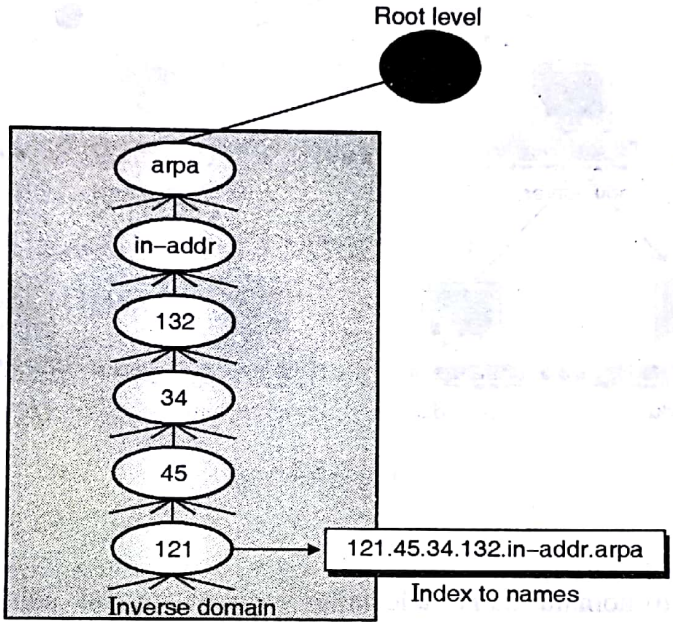


Fig. 5.3.5

5.3.5 Zone and Domains :

- Root server having authority of whole tree and also it keeps track of all the servers under each servers.
- A primary server loads all information about servers which are sub parts of it on the local disk file.
- The primary server has all the authority about the sub severs under it and also able to perform the operations like updation, modification, deletion etc.
- The secondary server loads all information from the primary server.
- It dose not have any authority to do any modifications in the information related with the server.
- When the primary downloads information from the secondary, it is called zone transfer.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

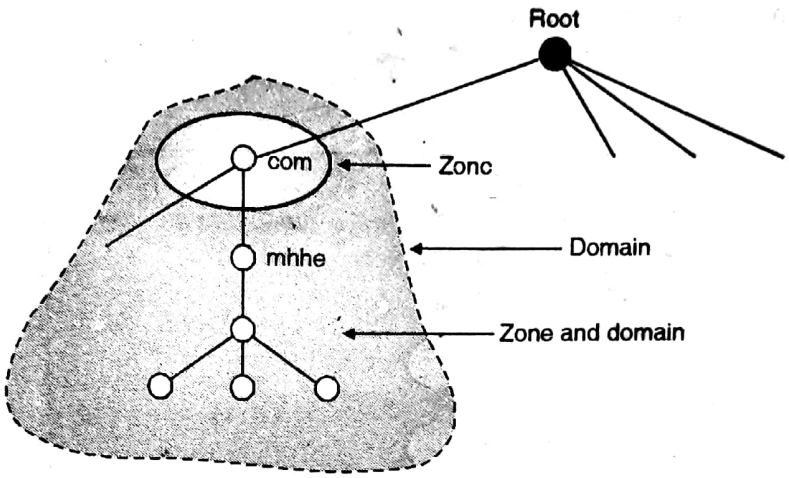


Fig. 5.3.6

5.3.6 DNS In the Internet :

Examples of top level domains :

1. Generic top level domains :

The generic domains are nothing but the registered hosts. It allows almost 14 possible labels which describes the organization types as listed below:

- .com - It defines commercial organization
- .org - Shows non profit organization
- .biz - Describes business or any commercial firm
- .gov - Explains government institutes
- .info - Defines information service provider
- .int - Shows international organization
- .edu - Describes educational institutes
- .aero - Airlines and aerospace companies are defined
- .mil - Describes about military group
- .name - Personal names are described
- .net - Network support system is explained
- .coop - Shows cooperative business organization
- .pro - Explain about professional organization
- .museum - Museums and other non-profit organizations are mentioned etc.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

For Example : chal.atc.fhda.edu

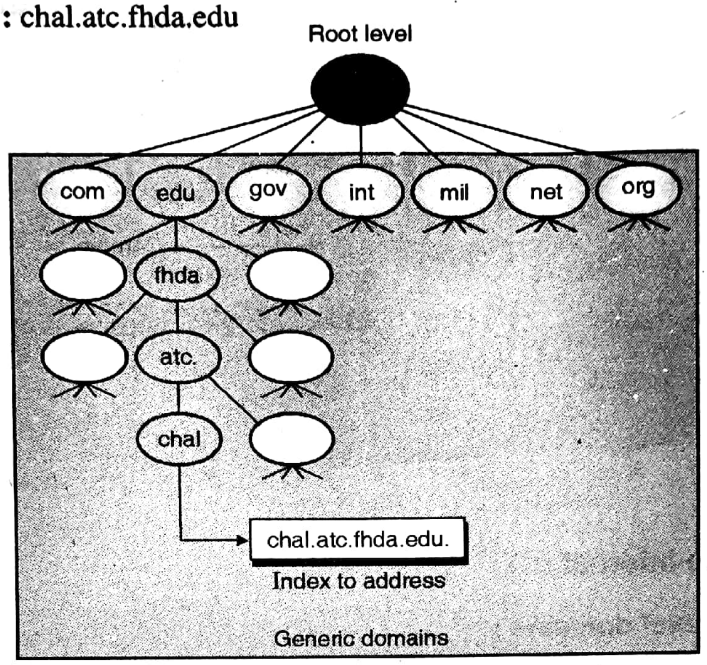


Fig. 5.3.7

2. **Country codes (2 character codes) :**

   It uses two characters from the name of the country.

3. **.jp, .in, .us, etc**

   For Example : anza.cup.ca.us

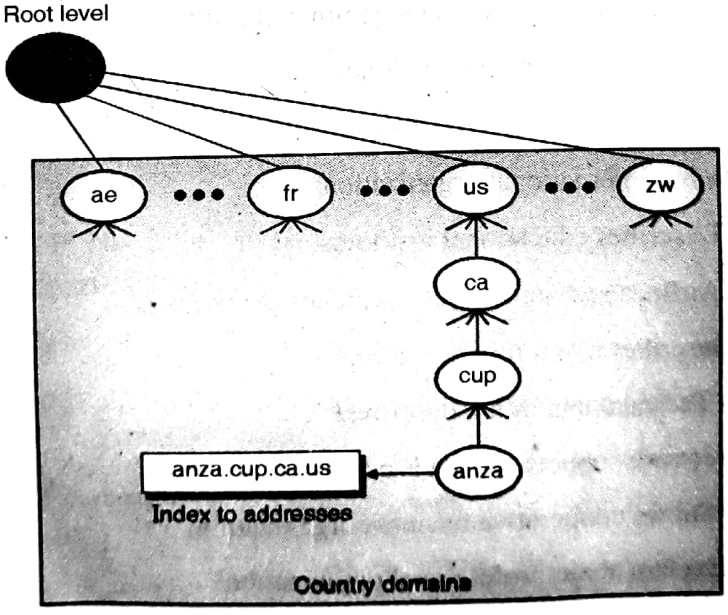


Fig. 5.3.8

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.3.7 How DNS Works ?

- The user adds URL in the address bar.
- From the URL client browser tries to get the domain name server where list of all the domain names along with their respective IP addresses are maintained.
- The domain name gives details like the IP address related with the particular domain name.
- Then name server sends reply to the client brouser along with the requsted web page's IP address.
- Then client brouser retrieves the required page from the specific IP address.

5.3.8 Resolution :

Q. What is meant by resolution in DNS ? Explain **MU – April 2013**

The resolutions which we use to trace the path from client to required server.It may map address to name or name to address by using the help of resolver.

(a) Resolver :

A host or DNS Client which helps to map an address to name or names to an address.

There are two types of resolutions :

(b) Recursive resolution :

- In this type of client starts searching for required server by following the listed domains.
- The client wants to send data over the internet to the destination *mcgraw.com* ; where *.com* is domain and *mcgraw* is a name of receiver's mail box.
- Client first ask to its neighbour about intended destination. If the system is the destination then it answers with the positive reply email by following the neighbours in the path; till it reaches to thelse it ask tio next parential neighboring node about required destination.
- When a particular system found the destination; the server sends positive response to the client by reward back on the same path.
- Finally client can connect to the respective server via following the same path.
- In this process client searches the destination by following the path in a sequence which reaches to the required destination.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

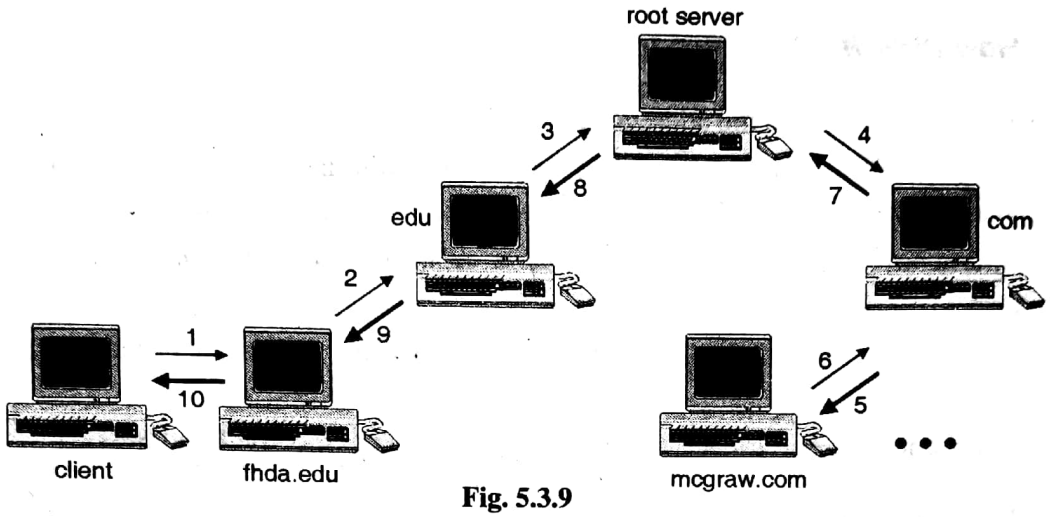


Fig. 5.3.9

(c) Interactive Resolution :

- Client start searching the respective server but client sends one-to-one message to check whether the current place is required server.
- The client ask for intended system if the receiver is required machine then search is completed and sends positive relpy.
- If client does not get positive reply from system then it sends ip address of another neighbor which can complete the search of client client.
- When it founds the required destination; the server sends positive reply then finally mail transfer takes place between client and server.

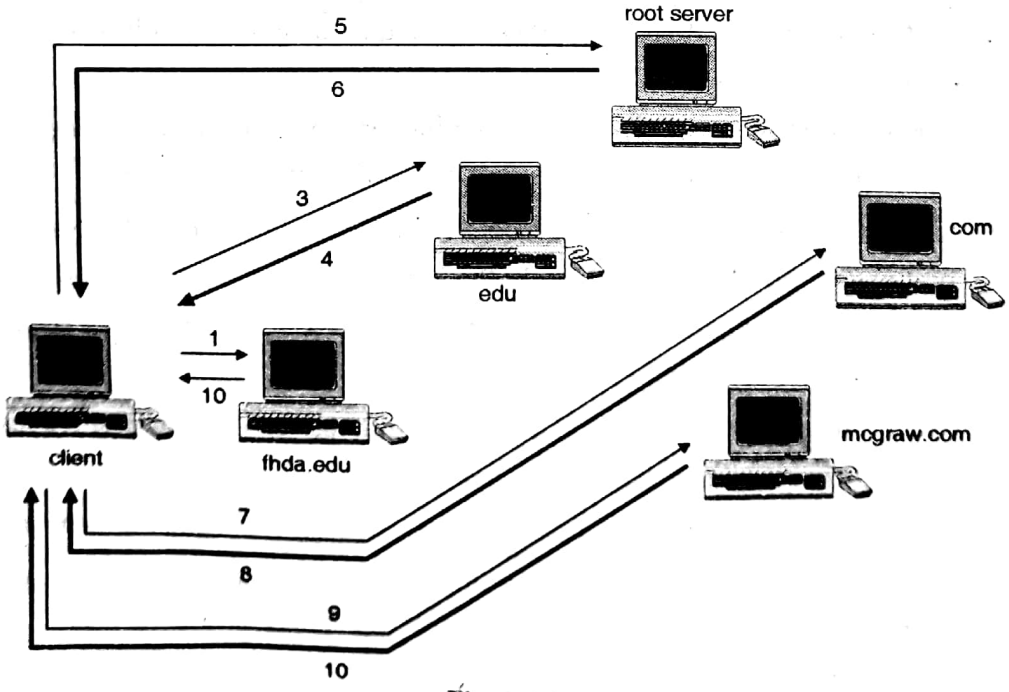


Fig. 5.3.10

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

5.3.9 DNS Messages :

There are two types of DNS messages :

1. Query
2. Response

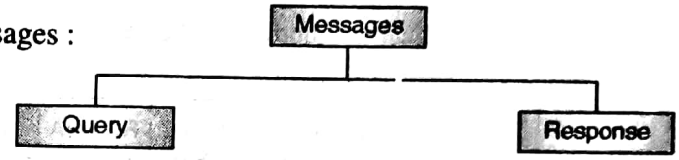


Fig. 5.3.11

(a) Query and Response Messages :

- Query message contains Header and Question Section
- Response message contains various sections like Header, Question section, Answer section, Authoritative section, Additional section.

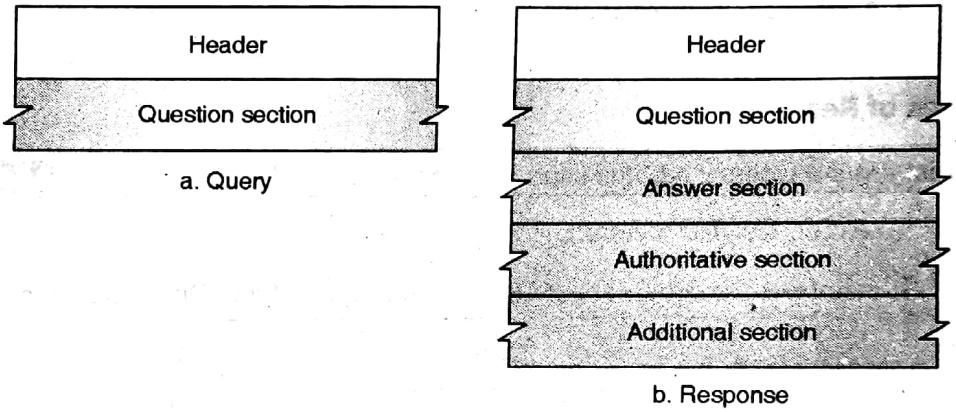


Fig. 5.3.12

(b) Header Format :

The Identification part maintains :

1. Number of question records
2. Number of authoritative records

The Flags maintains :

1. Number of answer records
2. Number of additional records.

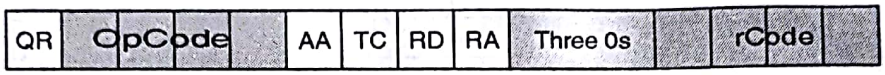
Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(c) Flags Field :

The fields of flags are mentioned below :



QR : Query/Response
OpCode : 0 standard, 1 inverse, 2 server status
AA : Authoritative
TC : Truncated
RD : Recursion Desired
RA : Recursion Available
rCode : Status of the error

(d) Types of Records :

Q. What are the types of records used in Domain Name System. **MU – April 2013**

1. Question Record format :

It maintains the details about Query Name, Query type, Query class etc.

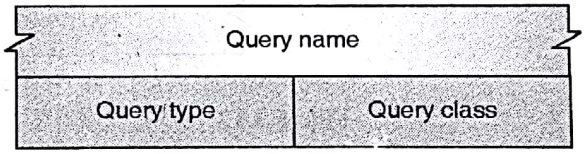
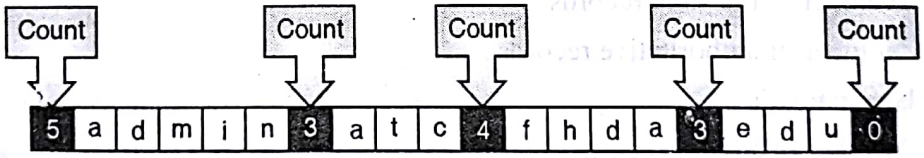


Fig. 5.3.13

2. Query name Format :



admin.atc.fhda

Fig. 5.3.14

Review Questions

Q. 1 Describe connections in SCTP what is association in SCTP?.

Q. 2 Write a chunks in SCTP.

Q. 3 Explain cookies in SCTP.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Q. 4 compare UDP TCP and SCTP.

Q. 5 Explain SCTP packet in detail.

Q. 6 Write a short note on DNS.

Q. 7 Explain various domains of name system.

Q. 8 Describe DNS header message.

Q. 9 Give DNS distribution of name space.

Q. 10 Explain name to address mapping using DNS.

Q. 11 What are two categories of DNS messages ?

Q. 12 How we can use DHCP.

Q. 13 What is need of DHCP protocol.

Q. 14 Explain working of DHCP server.

5.4 University Questions and Answers

April 2013

Q. 1 Explain the DHCP client transition diagram. **(Section 5.2.6)** **(5 Marks)**

Q. 2 What are the types of records used in Domain Name System.

(Sections 5.3.9(d)) **(5 Marks)**

Q. 3 What is meant by resolution in DNS ? Explain. **(Section 5.3.8)** **(5 Marks)**

Q. 4 Define and give example of the following

i. Fully qualified domain name

ii. Partially qualified domain name

(Section 5.3.2) **(5 Marks)**

Q. 5 Explain the features of Stream Control Transmission Protocol.

(Section 5.1.4) **(5 Marks)**

□□□

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Note

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

CHAPTER 6

Application Layer Protocols II

Syllabus :

- Remote Login : TELNET and SSH
- File Transfer: FTP and TFTP
- World Wide Web and HTTP

6.1 Remote Login

6.1.1 TELNET (Terminal Network) :

(a) Introduction :

- TELNET is general purpose client-server type application protocol useful in TCP-IP model for remote system communication.
- Communicate by transferring data and control characters (ASCII) format over the connection.
- TELNET client works on ephemeral (any available port) and TELNET server works on port 23.
- Remote login is useful for remote process access. It means it helps for communication with two remote systems.
- Remote login works as TCP-IP protocol follows client - server architecture on port 513.
- TELNET was innovated when operating systems where following time-sharing environment.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- In time sharing scenario user feels like it is working on dedicated system for accessing a resources, running application programs for other systems etc.

(b) Login :

- Since many users are related with each other via central server the security must be included via authenticated login.
- User can access information from the server by using individuals authenticated login id.
- User can login to the system using "username", "password".

Types of Login :

1) Local Login :

- To connect with any system in a network users have to provide his/her details to a local server.
- When users enters data using keyboard or any input device it is given to *terminal driver* of operating system.
- Then terminal drivers passes the accepted characters to the operating system and then finally given to the desired application program as shown in the Fig. 6.1.1.

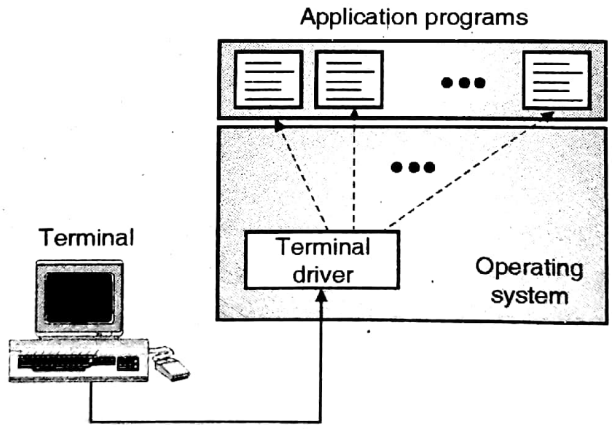


Fig. 6.1.1

2) Remote LOGIN :

- In the above case the user able to use the local applications.
- To connect with the applications running on the remote system can be done with the help of remote login as shown in the Fig. 6.1.2.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Client Side Login :

- The client sends data through input devices to the terminal driver.
- Then local operating system access it without interpreting it.
- The input characters are sent to the TELNET client to convert it into universal character set called as Network Virtual Terminal(NVT) Because of this the character set can be considered in standard format.
- This NVT set than given to TCP-IP stack at the client side.

Server Side Login :

- Than this set is forwarded over the internet and added to the TCP-IP stack at the remote side.
- This set is forwarded to operating system of remote machine but since it cannot interpret directly it is given to the TELNET server.
- From TELNET server it is given to pseudo terminal driver which gives proper interpretation and then forwarded via server side operating system to an appropriate application program.

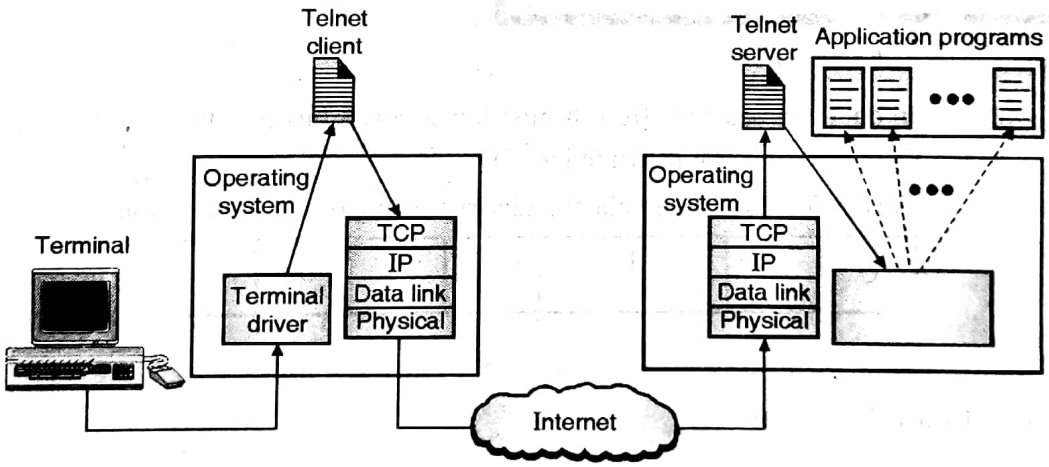


Fig. 6.1.2

(c) Network Virtual Terminal :

- Since in the network many heterogeneous systems are connected with each other individual system has its own operating system, terminal drivers etc.
- When client TELNET transfers the data over the internet to remote TELNET the character set considered by client machine is translated in Universal character set called as "Network Virtual Terminal" (NVT).

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Server TELNET than consider this NVT and transfer that into the format which is acceptable by remote machine.

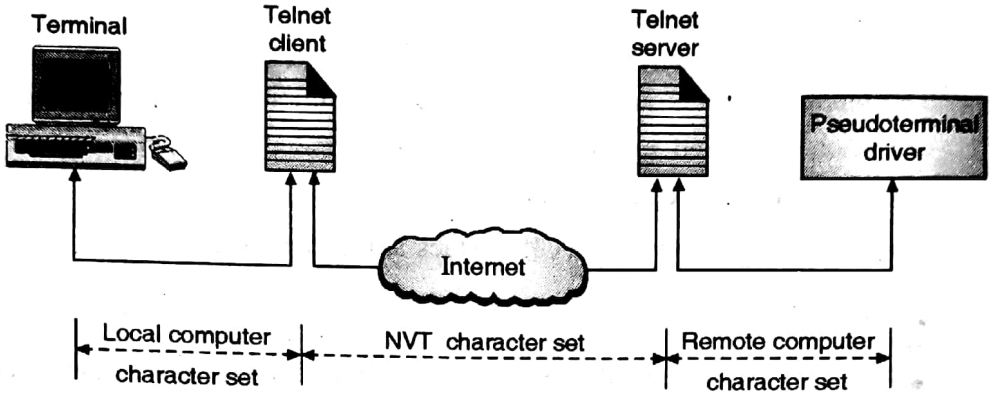


Fig. 6.1.3

(d) TELNET Character Set :

The NVT character considers two different character set :

(a) Data character set (8 bits)
(b) Control character set (8 bits)

(a) Data character set :

- In data character set from 8 bits; lower seven bits are the ASCII values and the highest bit is represented as "0".
- This is decided among client and server using option negotiation.

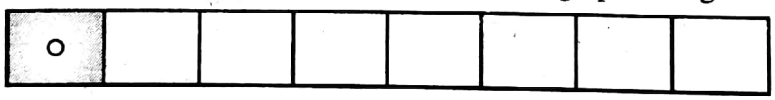


Fig. 6.1.4

(b) Control character set :

- In control character set from 8 bits; lower seven bits are the ASCII values and the highest bit is represented as "1"(just replacing 1 on place of 0 in above Fig. 6.1.4)
- Some examples of NVT control characters along with their binary representation;

  EOF (End Of File) : 11101100

  EOR (End Of Record) : 11101111

  NOP (No Operation) : 11110001

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

BRK (Break) : 1111011

IP (Interrupt process) : 11110100

(e) Embedding :

- The TELNET works on single connection of TCP.
- As mentioned earlier TELNET client uses ephemeral port and TELNET Server uses port 23.
- Since TELNET contains data and control character sets for distinguish between them special control characters are used like IAC (Interrupt As Control).

For example as given below:

Client sends: cat file1

the "cat" is unix command which helps to display the content.

Client sends: cat filea <backspace> 1

- It means the file name is wrongly printed as " filea" istead of "file1" by using backspace in the command this correction can be done at server side it is not possible to do st client side.
- The two control characters are added (embedded) in message instead of backspace the characters are "IAC" and "EC".

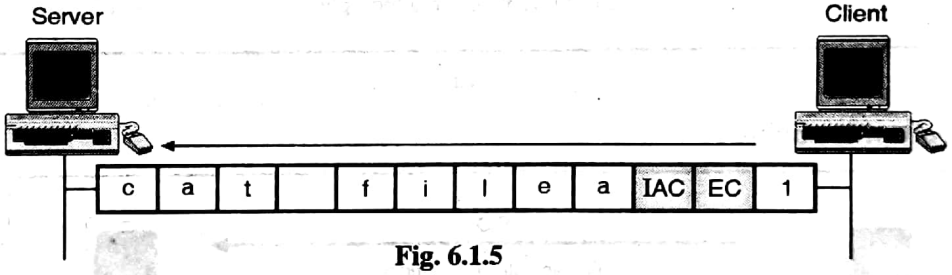


Fig. 6.1.5

(f) Options :

- To connect with the remote server and transfer data over it requires proper connection between client and server TELNET.
- Before the transmission of data both the ends negotiate options available and also the features available.
- Some examples of options are listed below;

0 – binary

useful for interpreting 8 bit data

1 – echo

display the data from one side to other.

5 – status

represents status of TELNET

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

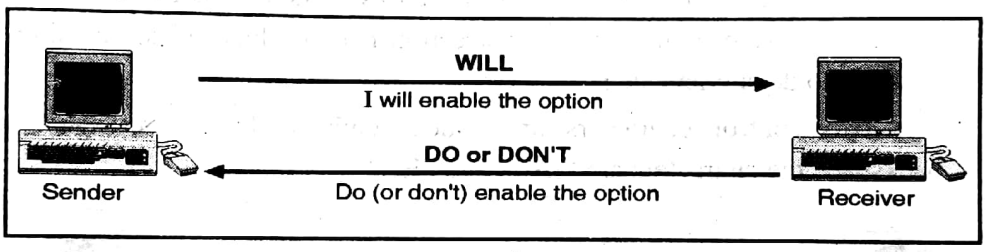
24 – terminal type
helps to represent Terminal type
34 – terminal speed
helps to represent Terminal speed

(g) Option Negotiation :

- Option negotiation plays an important in TELNET option setting.
- Four control characters along with their code and meanings are considered as follows;

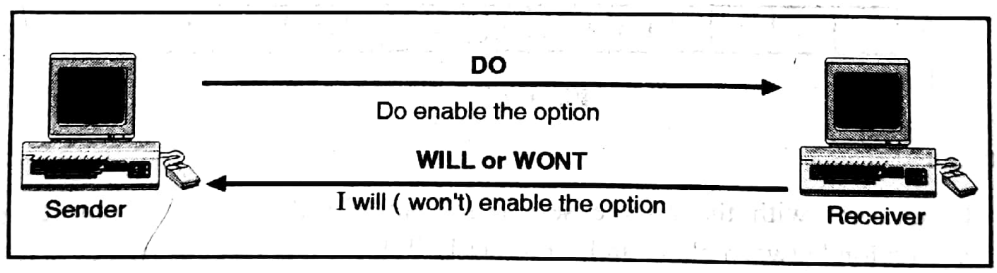
Will – 251	helps for offering to enable the options
Wont -252	represents that the enable of the options not possible
Do -253	It request for enabling the options
Dont -254	It rejects the selected option.

1. Offer to enable :



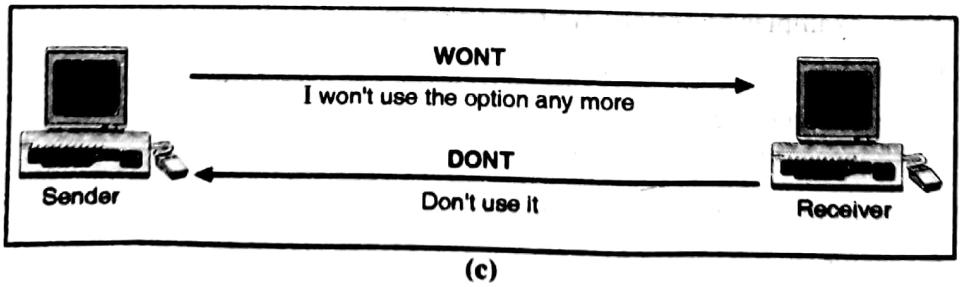
(a)

2. Request to enable :



(b)

3. Offer to disable :



(c)

Fig. 6.1.6

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Echo option example :

- By using IAC, Do and ECHO commands client ask for the considering the data transferred at sever side
- The echo option is available on server side is stated using Echo, Will and IAC signals.

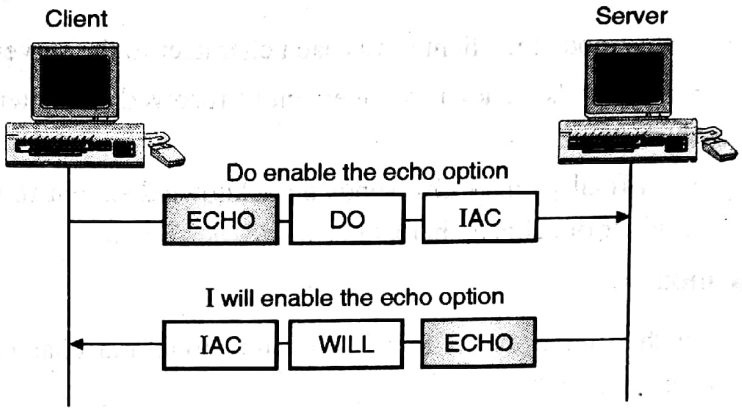


Fig. 6.1.7

Example of interrupting an application program :

- On local system applications aborted by user.
- But on remote system this should be done by using special control character i.e. IP (Interrupt Process).
- As we are able to see in the figure the interrupt is occurred using IP and then server sends aborted status to the application on server's side

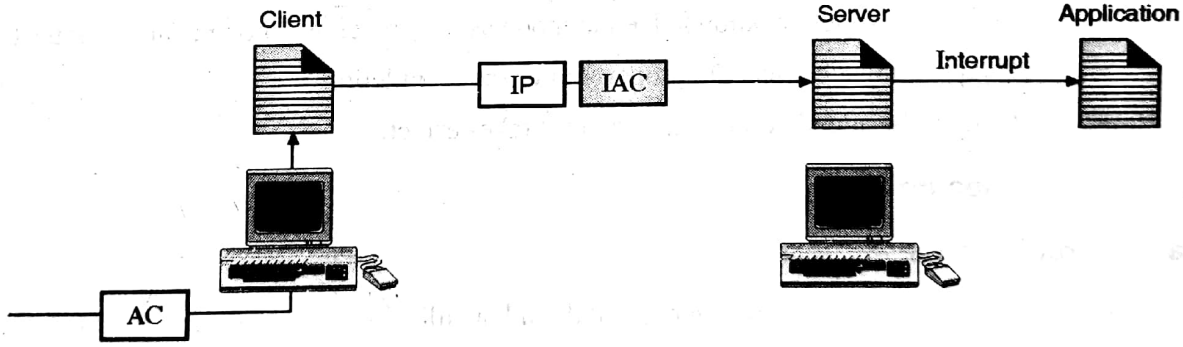


Fig. 6.1.8

(h) Modes of Operation

The modes of TELNET are as listed below;

(a) Default Mode

- This mode is used if no other mode is selected from the option negotiation.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The client sends a character till full line is completed and sends echo signal to server for displaying the data.
- The client waits for go ahead command from server. It works as half duplex mode.

(b) Character mode

- In this mode the client sends each character to the server.
- Server sends an acknowledgement of received character and echo's the sent character.
- Then finally client also sends an acknowledgement to the server about the receiver of echoed character.

(c) Line mode

- In this mode merits of both default mode and character mode combined together.
- In the line mode the whole line is sent by client to server only after editing.
- It is not as default mode because it does not wait for go ahead from server side
- It works as full duplex mode.

(i) The Rules of Negotiation :

The rules of negotiation are explained below;

- At the time of mode change the requests must be issued.
- The parties should acknowledge the mode as they receive a mode change request.
- A request must be inserted properly after the completion.
- It should be added at the place where it takes effect.

6.1.2 SSH (Secure Shell) :

(a) Introduction :

- Internet access has become a vital and available, it has become an essential replacement for traditional couriers, telephone, and fax, as well as remote dial-up access to a company's internal computer resources.
- One of the biggest challenge in using the Internet is security.
- Secure Shell is a protocol helps to provide authentication for secure users login, encryption for data security and data integrity to communicate with several users in the network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Secure Shell provides following facilities.
  - It provides file transfer which is secure, secure access of remote machines and also having own commands which provides secure programming
  - In the most popular operating systems secure shell client and server applications are widely available.
  - Securing data sent over a public network is offerd by secure shell.

(b) What is SSH ?

- SSH is a protocol for secure remote login and other secure network services over an insecure network.
- Developed by SSH Communications Security Corp., Finland
- It is useful as a standard for unencrypted unix utilities such as telnet, rlogin, and rsh.
- Agent which allows arbitrary TCP/IP to be forwarded over a secure channel.
- It is useful for entrusted hosts on insecure networks mostly when work from home facility is available.

Two distributions are available :

- Commercial version
- Free ware (www.openssh.com) : Specified in a set of Internet drafts

(c) Need :

- If user trust local users/ISP/Script ; then there is no requirement of SSH.
- If user uses protocols that can not be routed over SSH e.g. UDP based services or user's client machines don't support SSH; then no need of using SSH.
- Otherwise, SSH will benefit user's network.

(d) Working :

- For the security purpose many algorithms are available.
- The RSA public key cryptography algorithm is useful while connection establishment i.e. during handshake between client side and server side.

(e) Security Features :

It uses various algorithms for security purpose

Due to security algorithms; we are able to get,

- Authenticated login
- Secure connection between client – server

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Various encryption methods
- Secure access of remote data.

(f) Connection :

The data exchange in SSH takes place between client and server using TCP connection

- First we go for TCP connection setup.
- The client initiates the connection. The server listens on port 22.
- Exchange of SSH version string between client and server
- SSH version string exchange between client and server must end with " \CR \LF " .
- It is used to indicate the capabilities of an implementation triggers, compatibility extensions and current protocol version.
- Between client and server the exchange of SSH key takes place with the help of various algorithms after negotiation.
- All packets that follow the version string exchange is sent using the Binary Packet Protocol. The exchange of data takes place between client and server.
- After the fulfilment of requirement the TCP connection gets terminated between the client and sever.

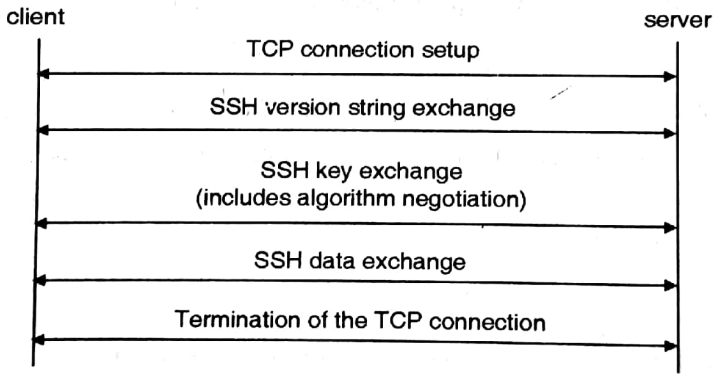


Fig. 6.1.9

6.2 File Transfer Protocols

6.2.1 FTP (File Transfer Protocol) :

(a) Introduction :

- FTP is a widely accepted Internet Standard.
- FTP follows standard client-server model. For successful FTP connection, there needs to exist both FTP *client side program* and FTP *server side program*.
- FTP Server: Store the files accessed during the file transfer

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- FTP Client: It send files or retrieve files by connecting to the FTP server.
- In the FTP when client sent request to server for particular file server sends response to client hence it is called as *"request and response model"*
- There are two mandatory two ways transmission connections in FTP

(b) Control connection (Command Control) :

- It keeps control between Client Control Processes and Server Control Processes during the communication
- Using Client side command for establishing the connection with the FTP server, sending FTP commands, receiving responses from the SERVER.
- Control Processes also known as Process Interpreter (PI) .
- It is also called as primary connection.
- The FTP uses the Telnet protocol on the control connection.
- By using this FTP client-server model; FTP client can transfer commands, which describe the functions to be performed, and the FTP Server replies to these commands.

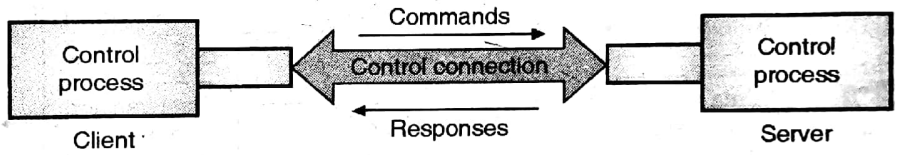


Fig. 6.2.1: Control Connection between Client-Server

(c) Data Connection :

- It helps to transfer require data between Client Processes and Server Processes during the communication.
- It is supportive for listening commands coming from a client over the control channel on a data port, establishing the connection for the control channel
- Receiving FTP commands from the client and responding them and running the SERVER commands.

(d) Data Transfer Process (DTP) :

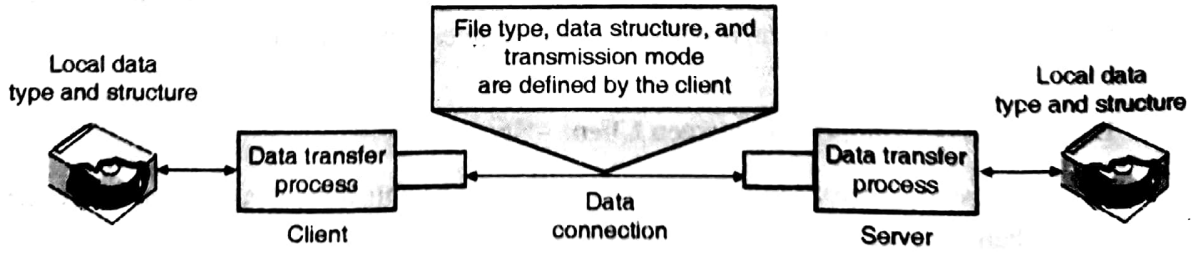


Fig. 6.2.2 : Data Connection between Client-Server

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- FTP works on TCP connection. It needs two TCP connections between client and server.
- The well-known *port 21* is used for the *control connection* and the well-known *port 20* for the *data connection.*
- Every FTP implementation must support the use of the default data ports, and only the USER-PI can initiate a change to non-default ports.
- Both the Client-server Data Transfer Processes have a default data port.
- The transferring of data consists of setting up the data connection to the appropriate ports and choosing the parameters for transfer.

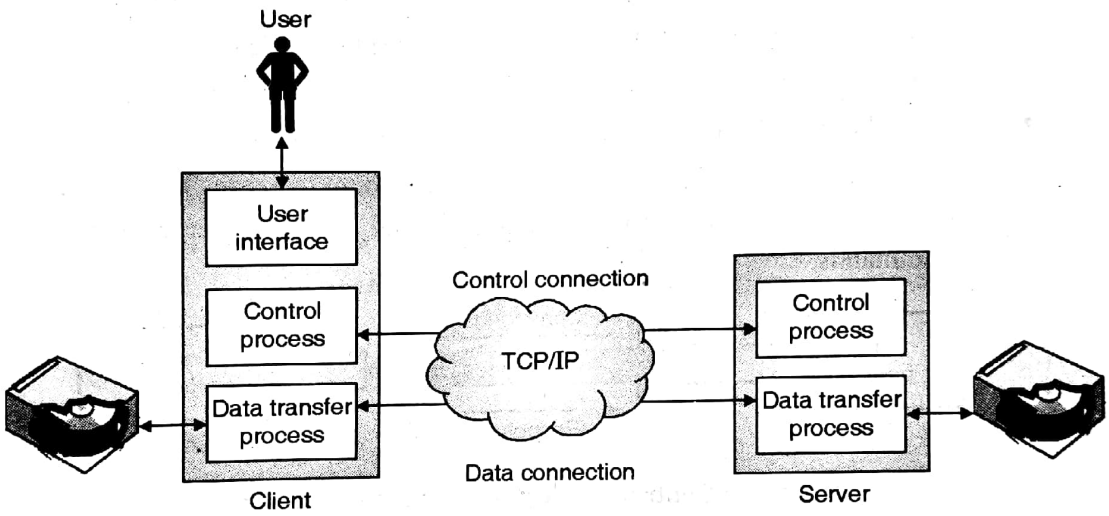


Fig. 6.2.3 : File Transfer Protocol between Client-Server

(e) Working of FTP :

Introduction :

- The client sends FTP commands to the server, the server interprets them, runs its DTP, then sends a standard response.
- Once the connection is established between client and server, the server-PI gives the port on which data will be sent to the client DTP.
- The client DTP then listens on the specified port for data coming from the server.
- After the data transmission is over the connection between client and server is terminated.

1. Control Connection between Client – Server :

By using control commands the connection establishment takes place between client and server.

www.MumbaiBScITStudy.Com

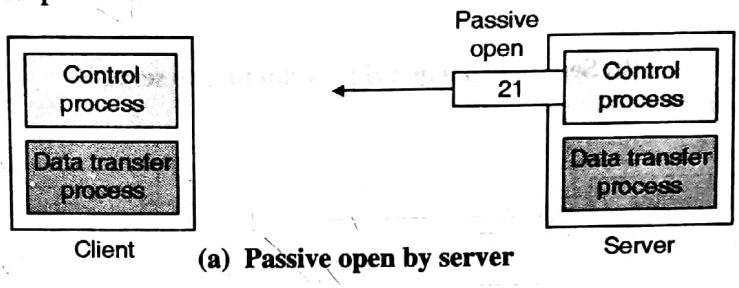
Mumbai B.Sc.IT Study

- **Passive Open by Server :**

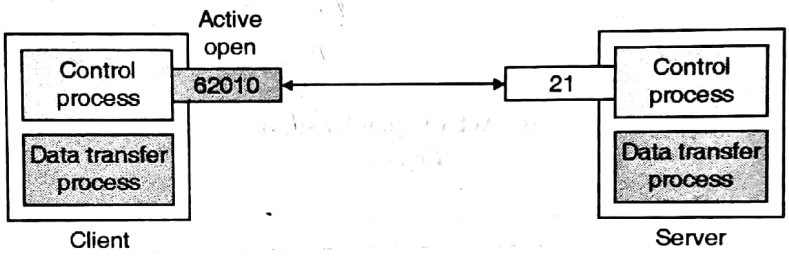
  As shown in the Fig. 6.2.4(a) firstly the Server will Passive opens the *Control connection* on default *port 21.*

- **Active Open by Client :**

  Then as shown in the Fig. 6.2.4(b) the Client actively opens the connection on port 62010.



(a) Passive open by server



(b) Active open by client

Fig. 6.2.4

2. Data Connection between Client – Server :

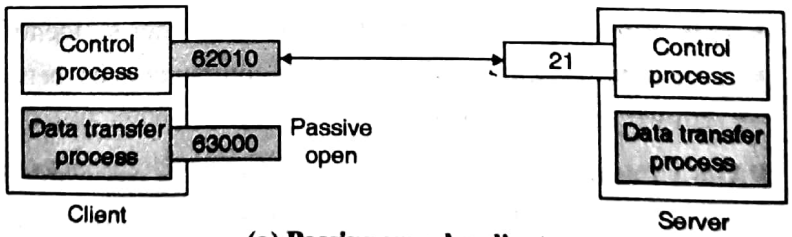
- **Passive Open by Client :**

  As shown in the Fig. 6.2.5(a) firstly the DTP passively opens port number 63000 for transferring the require data.

- **Active Open by Server ;**

  As shown in the Fig. 6.2.5(b) by using port 63000 Client sends ephemeral (temporary) port number to server for data transfer process.

  On default *port 20* client starts sending data to server using ***data connection.***

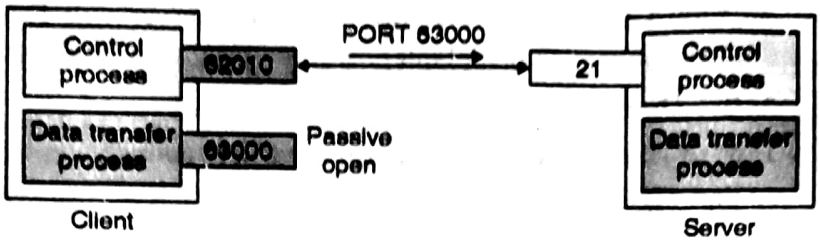


(a) Passive open by client

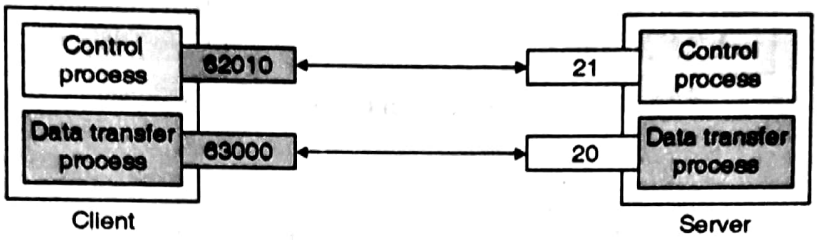
Fig. 6.2.5(cont...)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study



(b) Sending ephemeral port number to server



(c) Active open by server

Fig. 6.2.5

(f) FTP Commands :

Q. List any five file management commands of FTP and write their purpose

MU - April 2013

FTP commands specify:

- Used Port numbers
- Data transfer methods.
- Data structure
- The nature of the action to be conducted like Retrieve, List, Store, etc.
- There are three different types of FTP commands with some examples are listed below;

(a) Access control commands :

1. **USER** Character string useful for the user's identification. User identification is necessary to establish communication between client and server over the data channel.
2. **PASS (Password)** Character string gives user's password. This command followed by the USER command. We hide the display of this command for security reasons.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3. **CWD (Change Working Directory)** it allows the current directory to be changed.

   The directory's access path can be given as an argument in the command.

4. **QUIT** Command helps to terminate the current session. The server waits to finish the transfer but before closing the connection server checks for the need of client and response for the need.

(b) Transfer parameter commands :

1. **PORT** the port number can be specified using Character string.
2. **TYPE** Specifies the type of format in which the data will be sent is specified.
3. **STRU** It indicates the character indicating the file structure

   F for File, R for Record, P for Page
4. **MODE** It gives data transfer method

   S for Stream, B for Block, C for Compressed

(c) FTP service commands :

1. **RETR** It helps for retrieving copy of the file whose access path is given in the parameters from the server DTP
2. **STOR** It helps to accept the data sent over the data channel and store them in a file having the name given in the parameters.

   If the file does not exist with the mentioned name, the server creates it else overwrites it.
3. **DELE** (delete) It helps to delete a file. The name is given in the parameters.
4. **RMD** (remove directory) It enables a directory to be deleted whose name is indicated in the parameters.
5. **MKD** (make directory) It helps to create a directory . The name of the directory to be created is mentioned in the parameters.
6. **PWD** (print working directory) It is useful to resend the complete current directory path.
7. **NOOP** (no operations) It is only used, when there is a idle time between client and server in order not to be disconnect the connection.

(g) FTP Response :

- As we have seen FTP is request-response model; when server gets any request command it reply using FTP response mechanism.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- For each command from client; server try to answer it using appropriate response.
- The responses are made up of using 3 digit code.
- These 3 digit codes are difficult to remember by humans, hence it is accompanied by a text.
- The response codes are made up of 3 numbers the meanings of which are as follows :

1. **First digit :** It recognize the status of the response (success or fail)
   - **1yz Preliminary positive response:** It helps to mention the action requested is in progress
   - **2yz Positive fulfilment response:** It shows the status of action requested has been fulfilled, a new command can be sent.
   - **3yz Intermediary positive response:** It helps to show an action request is temporarily suspended. Additional information is awaited from the client.
   - **4yz Negative fulfilment response:** By using this response the client is requested to try again later. The previous action requested has not taken place because the command has temporarily not been accepted.
   - **5yz Permanent negative response:** This command helps to the client to formulate a different request. The command has not been accepted since the action requested has not taken place.
2. **Second digit :** It specifies what the response refers to.
   - **x0z Syntax** : It helps to give response like;The action has a syntax error or the command not understood by the server.
   - **x1z Information :** This response sends back an information for example a response to a STAT command.
   - **x2z Connections**: It shows the response related to the data channel.
   - **x3z Authentication and accounts :** It helps to show the response related to the login or the request to change the account.
   - **x4z File-transfer-protocol does not use this response.**
   - **x5z File system :** This is the response related to the remote file system.
3. **Third digit :** It provides a more specific meaning relative to each second digit.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(h) FTP Code examples :

FTP reply codes are listed below:

FTP Reply Codes

Code	Description
110	Restart marker
120	Service ready in minutes
125	Transfer starting since data connection already open
150	About to open data connection since File status is " OK"
200	Command "OK"
202	Command is not implemented on this host
211	System status or help
212	Mentions Directory status
213	Specify File status
214	Gives Help message
215	Virtual Memory is the operating system of this server
220	For new user the service is ready
221	Mentions the QUIT command
226	If requested file operations are successful the closing data connection takes place
227	FTP server has opened a passive connection at the specified IP address and port for data transfer
230	User logged on but requested mini disk, BFS, or SFS Directory not available to proceed
234	Secure data exchange complete
250	Requested file action or directory status is "OK"
255	The reply is in target directory already
257	Directory status given along with that PATH NAME created
331	Ask for password
332	Using account it supplies the mini disk password
421	Closing connection because service not available
425	Cannot open data connection
426	Transfer ended abnormally and Connection closed
431	Temporarily not able to process security

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Code	Description
450	Requested action not executed because of reasons like file busy, mini disks or SFS directory not available
451	Local error in processing since the requested action aborted
452	Requested action not taken due to insufficient storage space in system
500	Command unrecognized because of Syntax error
501	There is Syntax error in parameters or arguments
502	Not implemented the command
503	Exists a bad sequence of commands
504	Command not implemented for a particular parameter
521	With this PROT setting data connection cannot be opened
530	Indicates the status as Not logged on
532	Accounting is done for storing files
533	For policy reasons the command protection level denied
534	For policy reasons request denied
550	Requested action not taken since file not found or no access for specific files
551	Requested action aborted due to page type unknown
552	Since exceeded storage allocation requested file action ended abnormally
553	Requested action not taken since the given file name is not allowed

6.2.2 TFTP (Trivial File Transfer Protocol) :

(a) Introduction :

- TFTP is the Trivial File Transfer Protocol.
- TFTP uses UDP which is connectionless approach to make it simple and small while File Transfer Protocol (FTP), which uses TCP.
- TFTP does not require authentication means no need of LOGIN while dealing with it; hence we can say TFTP is less secure protocol.
- Implementation of TFTP requires UDP, IP, and a device driver can fit on **read-only memory.**
- TFTP is also useful enough for diskless workstations but only for few Kbyte code.
- It helps to download boot code from diskless workstations.
- The exchange between client-server takes place from the server only because the server can read or write a file for client.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

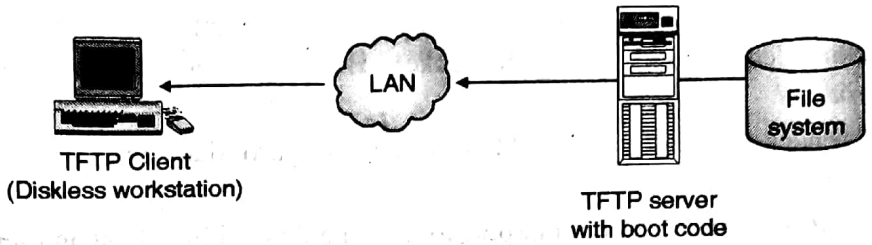


Fig. 6.2.6 : TFTP Client-Server Model

(b) Message Types :

Q. What are the types of TFTP messages? What is the purpose of each one? MU - April 2013

- There are five types of messages;
  1. Read Request (RRQ)
  2. Write Request (WRQ)
  3. Data
  4. ACK (acknowledgment)
  5. Error messages
- Some error codes are as follows :

  0 - not defined

  1 - File not found

  2 - Access violation

  3 - Disk full

  4 - Illegal TFTP operation

  5 - Unknown port

  6 - File already exists

  7 - No such user
- Each and every message format has 2 bytes reserved for OpCode (Operation Code)
- The filename specifies the file **on the server** that the client wants to **read from or** write to.
- The Modes are netascii or octet

  netascii : It is useful for transferring text files.
  All lines end with \r\n (CR, LF).
  Provides standard format for transferring text files.

  octet : It is useful for transferring binary files.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(c) TFTP Packet Formats :

- TFTP has only positive acknowledge correctly received packets are acknowledged with an ACK packet. Hence we can call it as *request-reply protocol.*
- If sender does not receive ACK packet in appropriate time it re-sends the last DATA packet.
- TFTP uses port 69 as default port for sharing data within client and server.

→ Packet layout :

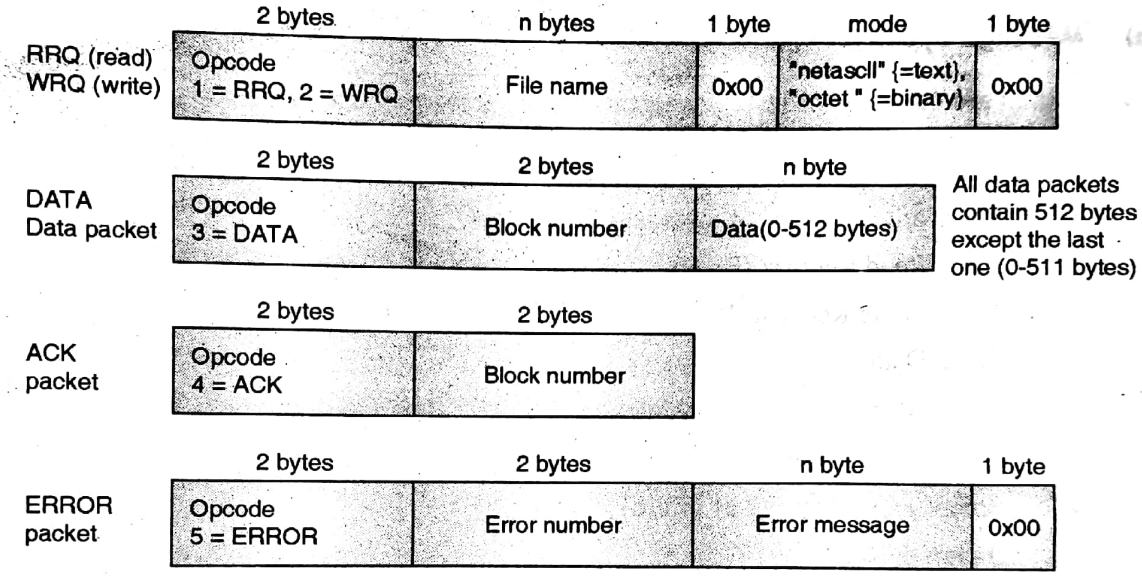


Fig. 6.2.7 : TFTP packet Format

(d) Read Request and Write Request Connections :

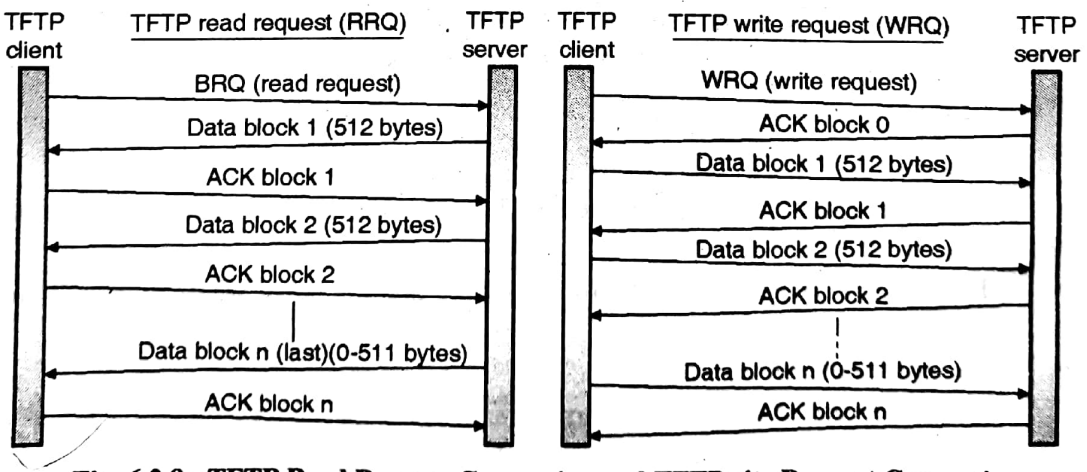


Fig. 6.2.8 : TFTP Read Request Connection and TFTP rite Request Connection

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(e) TFTP Example :

- As shown in the Fig. 6.2.9 the connection can be established between client and server for data sharing.
- By using main message formats this communication takes place.

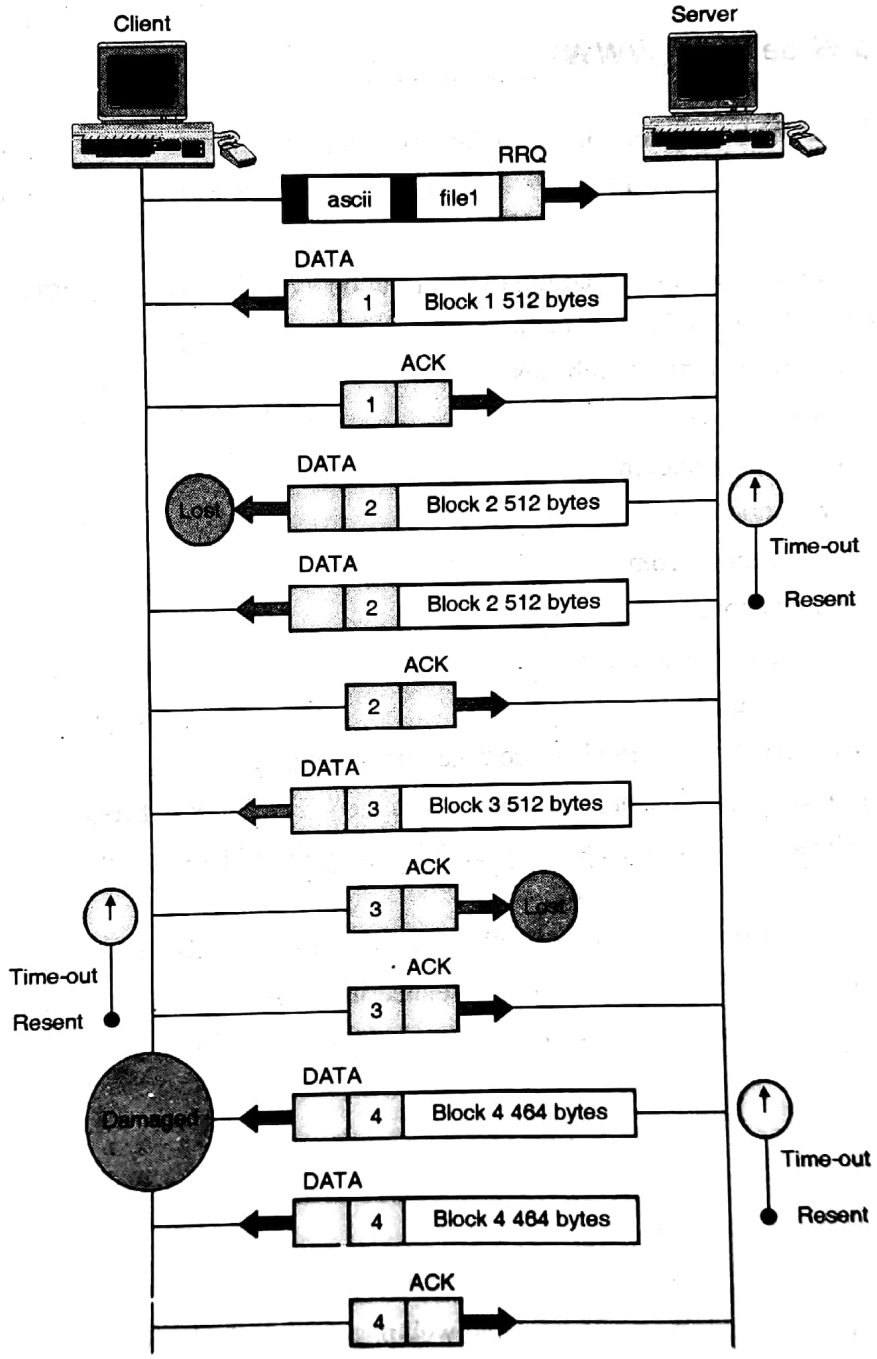


Fig. 6.2.9

- The ERROR message can be due to lost packets, checksum errors.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Lost Data Packets :

- Sender uses a timeout with retransmission.
- Sender could be client or server.
- Duplicate data packets must be recognized and ACK retransmitted.

6.3 World Wide Web (WWW)

- World Wide Web is system of interlinked hypertext documents accessed via Internet.
- Web is collection of useful information and related resources interconnected via hyper links.
- World Wide Web is vast collection of information available on the Internet, which gives data about any point at any moment.
- For example some famous websites are:
  - www.google.com
  - www.wikipedia.com
  - www.yahoo.com
  - www.facebook.com
  - www.irtc.com
  - www.w3school.com etc.

  Web pages contains :
  - **Text :** Number of simple or complex documents.
  - **Images :** The information also contains the various types of related images.
  - **Videos :** The documents may also includes the videos which are related to the topic.
  - **Multimedia :** The documents also contains flash, sounds etc.
- The Internet is really helpful for getting related information at only on a single click and without any hard work. The information can be used for a many of applications.

  For example :
  - WWW
  - Email
  - Instant messaging

  WWW provides information accesses in many ways are listed below :
- Hyper linked i.e. Hypertext : The related web pages are linked with each other.
- Graphical user interface : The front screen of any application.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Pictorial and non-text information : The images, videos, sound files are included in the web pages for better clarity about the particular data.
- Information that changes rapidly : The news flash, the weather forecast etc are updated instantly on web.
- Immediate access : The WWW provides immediate access of any web site on a click.
- Anyone can author a web site : As someone ready with new application he/she can launched it via launching the web site.
- Multi-user access to the same information (try that with a book)
- Easily search able information : Since information of particular point as well as the other related data we are able to search with the help of web pages over the Internet.

The functionality of the WWW is based on 3 main standards:

- URL (Universal Resource Locater)
- HTML (Hypertext Mark-up Language)
- HTTP (Hypertext Transfer Protocol)

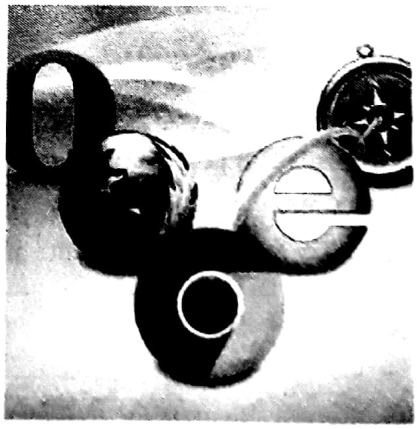
6.3.1 The Major parts of WWW :

(a) Web Pages :

- Large numbers of documents which are part of WWW are called as Web Pages.
- Most of the documents are constructed, designed and written using special languages called as "HTML" i.e. Hyper Text Mark-up Language.

b) Web Browser :

- Users can view the information available on the web through the software programs called "Web Browsers".
- Some examples of web browsers are as follows :
  - Netscape Navigator
  - Internet Explorer
  - Opera
  - Chrome



www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

c) Hyperlink :

The WWW content can be navigated by clicking the hyper links i.e. the Underlined or **Boldfaced words,** icons or images on the web pages.

d) URL (Uniform Resource Locator) :

- Each page of information on the web has a unique address called **the URL by** which it can be found.
- It is also known as web address.
- It is useful by browsers to locate a particular website form the large **number of** data available.
- There is difference between URL and Email address.
- Example of URL: http://google.com
- URL provides address of website which user wants to access .
- Example of Email Address: xyz12@gmail.com
- The email address is related with an individual and it helpful for storing emails.

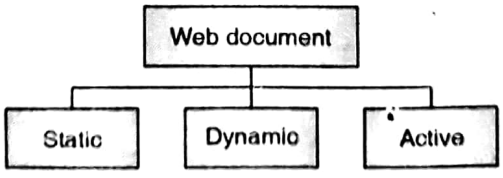
Sample examples of URL or Internet Addresses are as follows :

.com	Commercial site
.edu	Educational site
.net	Network organization site
.org	Not for profit organization
.gov	Government agency , department site
.mil	Military site

6.3.2 Categories of Web Documents :

Q. What are the types of Web documents **MU - April 2013**

- On the web we get large information accommodated in the web pages. These documents are information providers. These web documents provides lots of vital information about intended topic.
- These web pages or documents are classified based on their working as follows:

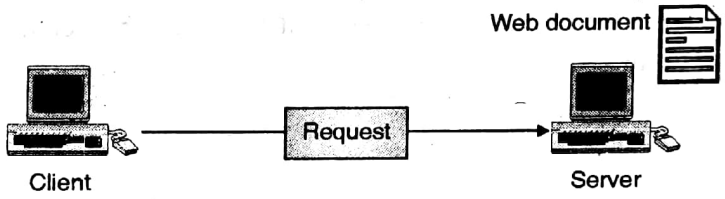


www.MumbaiBScITStudy.Com

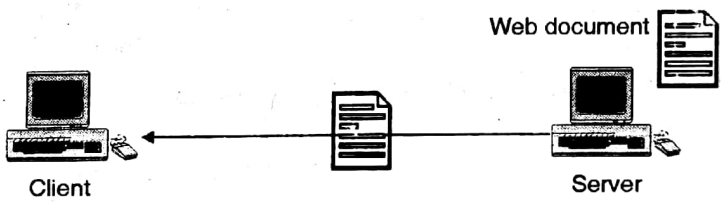
Mumbai B.Sc.IT Study

(a) Static Document :

- The static categories of web document are shown in the given figure.
- The client sends a request of required web document to server.
- Server searches the required web document in the databases.
- Server sends the requested web page as a response to the client.
- The contents remains same on the web server, each request for a static document results in exactly the same response.
- It is simple but inflexible.
- For example home page of any website like www.gmail.com. Whenever we will request the login page the user interface remains as it is.



(a) Request
Fig. 6.3.1



(b) Response
Fig. 6.3.2

The HTML is basic example of static web document which is helpful over the internet for transferring any kind of document. It is basically useful for static documents which contains useful information's.

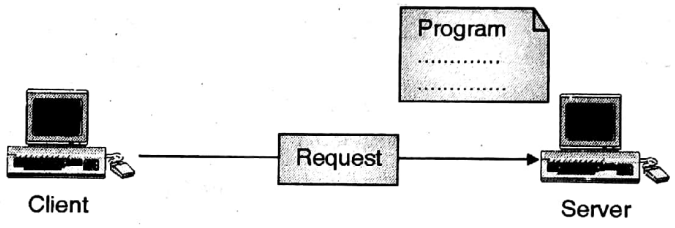
(b) Dynamic Document :

- In the static document; server responses with the saved static document to the client.
- A dynamic web document does not exist in a predefined form.
- The dynamic categories of web document are shown in the Fig. 6.3.3.
- The client sends a request of required document to server.
- The web server runs an application program that creates the document. Server executes the requested program and generates the output document.

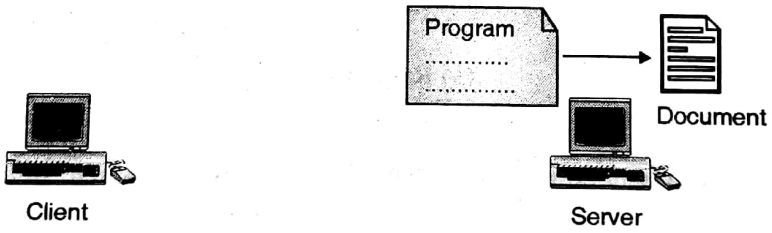
www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

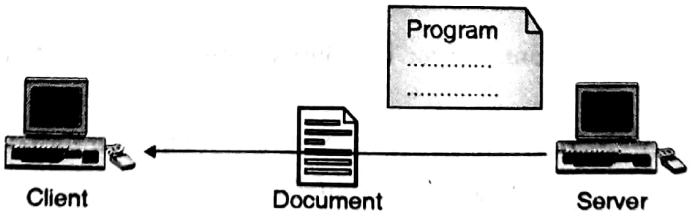
- The document generated by server mostly in HTML format forwarded to client system as a response for the display.
- The contents of a dynamic document can vary from one request to another.
- Dynamic web page covers any web page generated differently for each user like the online shopping site.
- The user browse through the site and ask for his/her required items then server replies with the specific and related information via a web documents. These documents various from user to user.
- The dynamic documents includes pages produced by client-side scripting, and created by server-side scripting such as ASP,JSP,ASP. NET,PHP etc where the web server generates content before responding it to the client.
- It gives current information to the client but once the documents retrieved the content cannot be changed.



(a) Request for running a program



(b) Running the program and creating the document



(c) Response

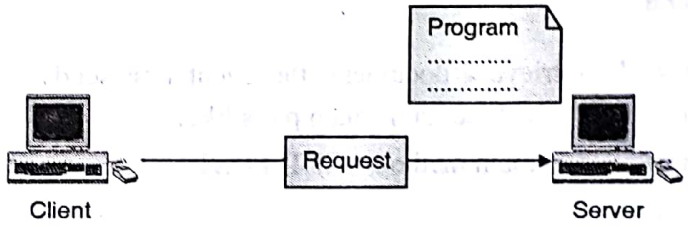
Fig. 6.3.3 : Dynamic Document

www.MumbaiBScITStudy.Com

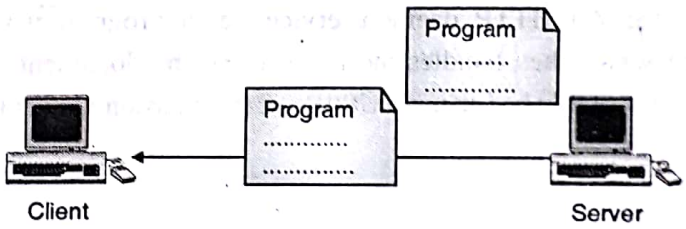
Mumbai B.Sc.IT Study

(c) Active Documents :

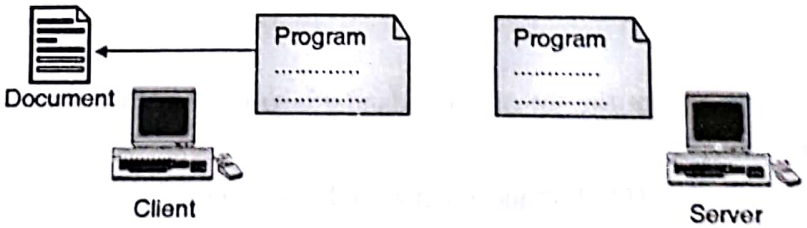
- The Microsoft Office is an example of an active document container.
- For example, a Microsoft Office contains Word documents, Power Point files, Excel spreadsheets, and so on.
- An active document can access sources of information directly and update the display continuously.
- Active documents require more sophisticated browser along with a powerful computer system to run the browser.
- For example In the case of Java programs the source code is translated in the byte code format and then sent to the browser and locally executed by the Java interpreter (JVM).
- Active categories of web document are shown in the Fig. 6.3.4.
- The client sends a request of required program to server.
- The web server searches the requested program in the repository and sends back the copy to the client.
- The client runs an application program and generates the required document and displays it.



(a) Request for a copy of a program



(b) Sending a copy of the program



(c) Running the program and creating the document

Fig. 6.3.4 : Active Document

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

6.4 HTTP

- For transmission of the web pages over the Internet HTTP protocol is very helpful which gives some rules to be followed while doing the flawless transmission of the web documents.
- The standard Web transfer protocol is HTTP (Hyper Text Transfer Protocols). It is used for document exchange between servers and clients on the web.
- It follows client-server model in the HTTP Request- HTTP Response pattern.

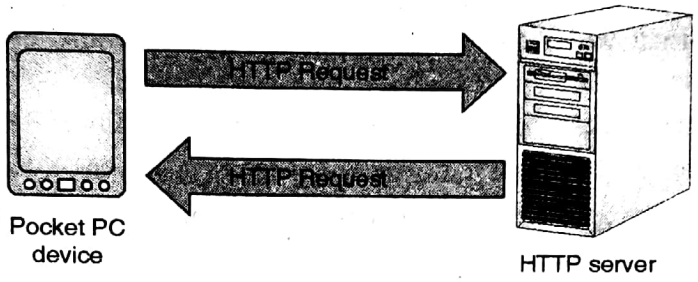


Fig. 6.4.1

6.4.1 How it Works :

- **HTTP Request:** To retrieve a document, the client first sends a request to the web server and waits for a reply. It contains main parts like;
  - Request line uses two main methods: GET, POST
  - Header lines
  - Request body (empty here)
- **HTTP Response:** An HTTP daemon/service i.e. a program which waits for Http requests on the server then handles the request and the document is sent to the client over a connection established using TCP/IP – Transmission Control Protocol / Internet Protocol.
- It contains main parts like :
  - Status line
  - Header lines
  - Response body
- Protocol is nothing but the set of rules/standards which we follow for communicating over the Internet.
  - The client sends a HTTP request using GET/Post method.
  - The server replies with a HTML document related with the users requirement.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

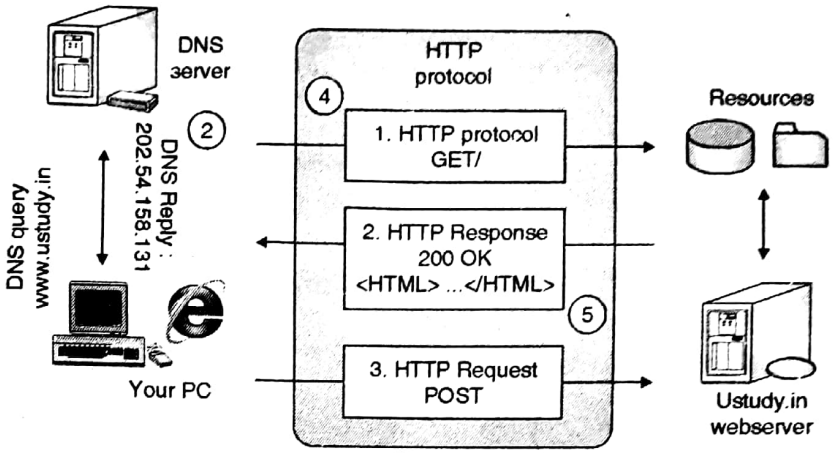


Fig. 6.4.2

6.4.2 Difference between GET and POST :

GET Method :

- In this method URL specifies all the name value pairs are submitted as a query string with the help of special characters.
- The name-value is not protected as it is visible in plain text format in the location bar of the web browser.
- We have to take special care for encoding data if special characters like ampersand (&) etc are present in the GET method since already the name-value displayed using the special characters.
- Length of the string is restricted in the GET method. We are not able to pass the data with large memory.
- GET is the default method; if method is not mentioned in the form tag.
- Data is always submitted in the form of text over the Internet using GET method.

POST Method :

- All the name-value pairs are submitted in the Message Body of the request not considered in the location bar of the URL.
- Post Method is secured because Name-Value pairs cannot be seen in location bar of the web browser.
- If the service associated with the processing of a form has side effects for example, modification of a database or subscription to a service; then the method should be POST.
- Length of the string i.e. the amount of data submitted is not restricted.
- Data is submitted in the form as specified in encryption type attribute of form tag.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Limitations :

- **Stateless :** HTTP is stateless protocol means it does not keep any information for future use.
- **Security :** No built-in security mechanisms is added in the HTTP protocol.
- It has built-in support for tracking clients session for the management

Review Questions

Q. 1 Explain different type of web documents.

Q. 2 Describe WWW and how email system works.

Q. 3 Write a short note on HTTP.

6.5 University Questions and Answers

April 2013

Q. 1 What are the types of TFTP messages? What is the purpose of each one?. **(Section 6.2.2(b))** **(5 Marks)**

Q. 2 List any five file management commands of FTP and write their purpose. **(5 Marks)**
(Sections 6.2.1(f))

Q. 3 What are the types of Web documents **(Section 6.3.2)** **(5 Marks)**

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

CHAPTER 7

E Mail Protocols

Syllabus

- Electronic Mail:
- SMTP, POP, IMAP and MIME
- Multimedia

7.1 Electronic Mail

1. Introduction :

- With help of web pages and HTTP protocol we can send an electronic-mail.
- These e-mails are sent between client and server over the World Wide Web using some protocols.
- These protocols helps to transfer the messages from client to server and also by using some protocols servers are able to retrieve and transfer e-mails.
- Some major protocols are explained in this point along with their working.
- Electronic mail requires several applications and services like Application layer protocols to transfer over the Internet ;
  1. Simple Mail Transfer Protocol (SMTP) - sending email
  2. Post Office Protocol (POP/POP3) - retrieving email

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

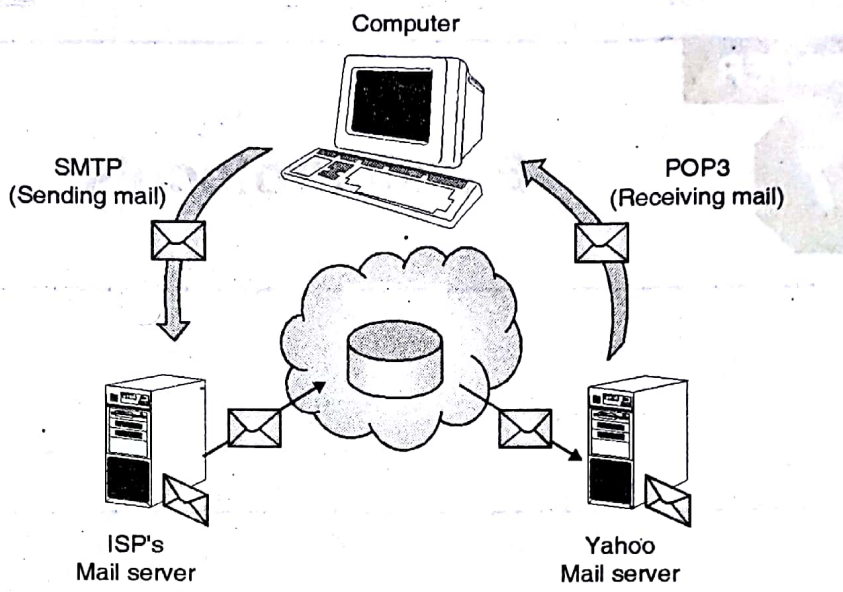


Fig. 7.1.1 : Role of various protocols in email transfer

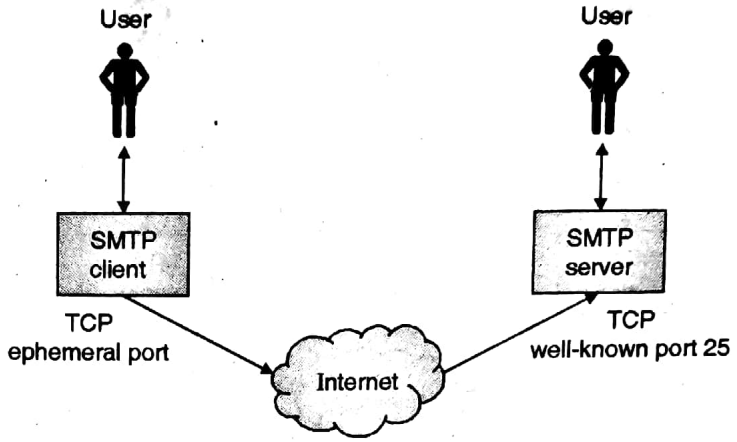
1. **Working :**
   - With help of web pages and HTTP protocol we can send an electronic-mail.
   - Electronic mail requires several applications and services to transfer the electronic mail over the Internet,
2. **Role of various protocols in service :**
   a) Simple Mail Transfer Protocol (SMTP) - sending email
   b) Post Office Protocol (POP/POP3) - retrieving email
   c) Hyper Text Transfer Protocol (HTTP) - world wide web

7.2 SMTP (Simple Mail Transfer Protocol)

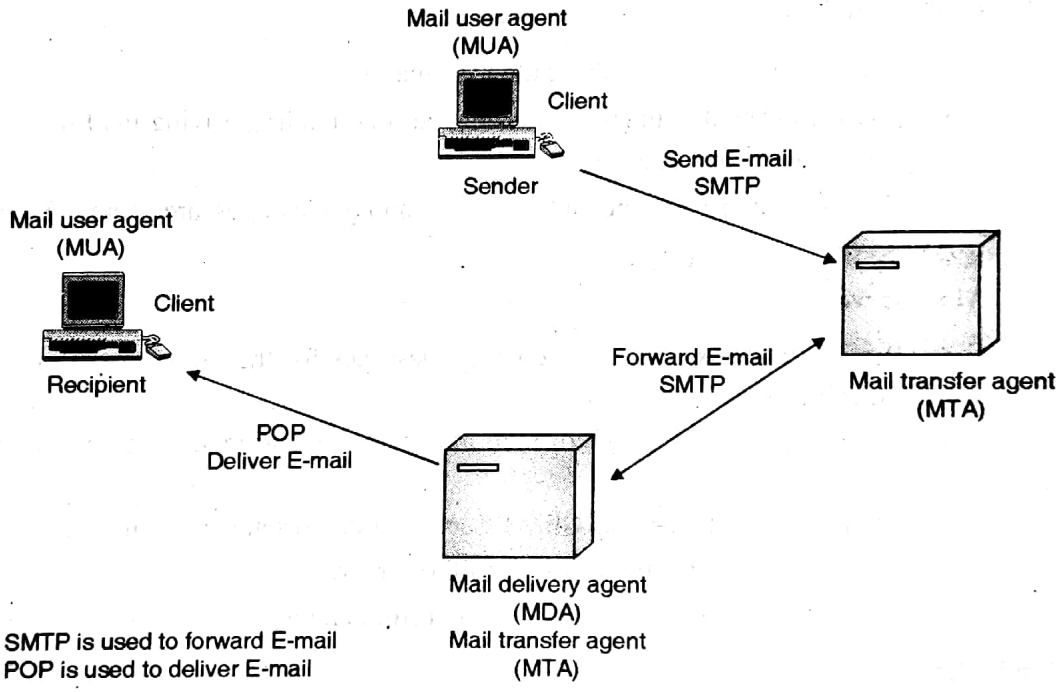
1. SMTP stands for Simple Mail Transfer Protocol is designed to be a very simple process to connect and read mail.
2. Simple Mail Transfer Protocol it is a standard application layer protocol for Electronic mail transfer while sending electronic mail.
3. This process designed to be used over the Internet; when the Internet was young and when the primary purpose of the Internet was to provide a way to share documents and information.
   (i) It works on well known port 25 by using Transmission Control Protocol (TCP).
   (ii) It uses Commands and responses encoded in ASCII in the form of Client-Server model.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study



(a)



(b)

Fig. 7.2.1 : Simple mail transfer protocol

(a) SMTP Components :

Q. Explain the user agent component of electronic mail system. MU - April 2013

1. User agents
2. Mail servers

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

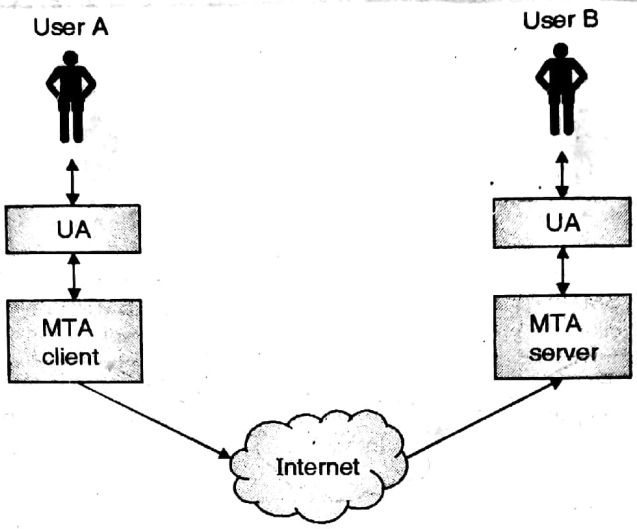


Fig. 7.2.2

1. **User Agent :**
   - User Agents (UA) are also called as "mail reader".
   - The User Agent handles composing, editing, reading, saving mail messages e.g. Outlook, Mozilla
   - On the mail server the outgoing, incoming messages are stored on mail server
2. **Mail Servers :**
   - Servers mailbox contains incoming messages for the user from the remote machine.
   - Outgoing message queue of mail messages are also maintained on the mail server.
   - SMTP protocol works as Client- Server model to send email messages
     (i) Client helps for sending mail to server.
     (ii) Server helps for receiving mail from client.

(b) SMTP Services :

The e-mail server operates two separate processes:

1. Mail Transfer Agent (MTA) is a process which is used for forwarding e-mail from client MTA to Server MTA on the local server.
2. The Mail Deliver Agent (MDA) can solve final delivery problems, such as virus scanning, Spam filtering, and return-receipt handling.

- Mail User Agent i.e. Client sends an email to server recipient@domain.com
- Client is connected to many servers at the same time.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- First it will confirm from server that whether the needed servers mail box exist or not.
- If the needed servers mailbox does not exist then client will search on other servers till getting the needed server.
- After getting the server client will transfer the mail via TCP connection to the server's mail box.

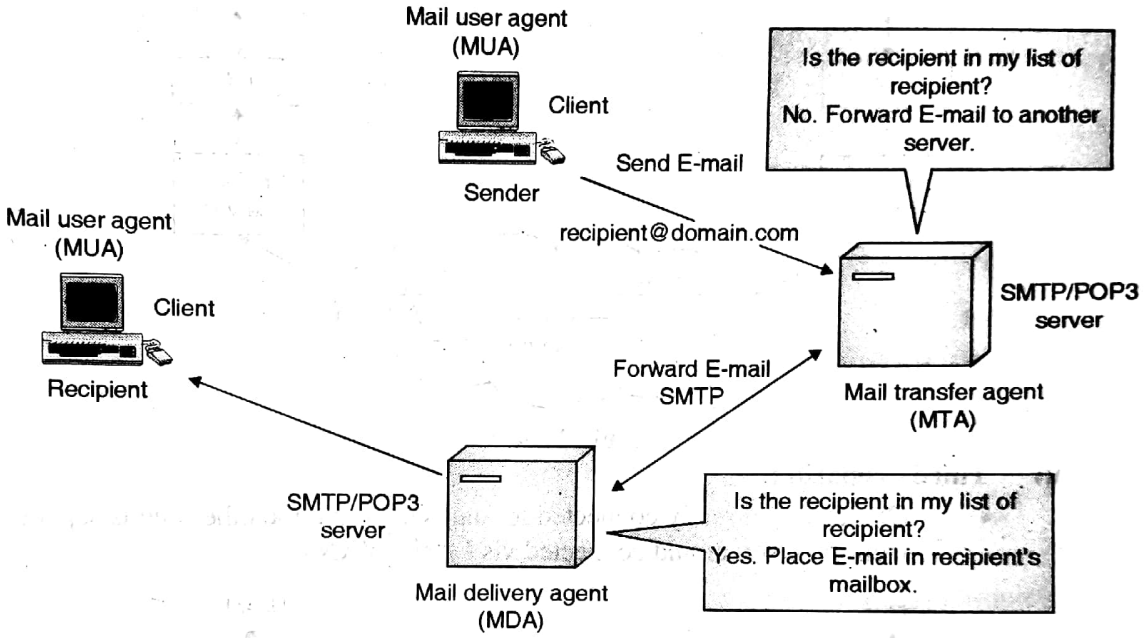
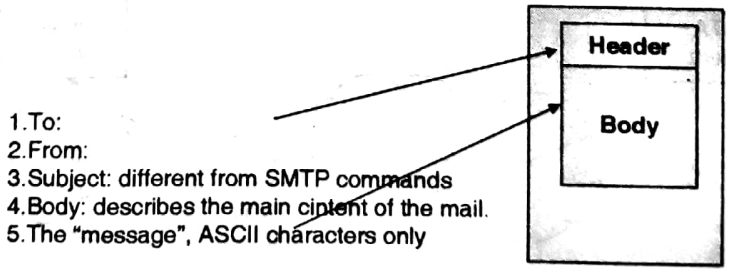


Fig. 7.2.3 : Email server-MDA

(c) SMTP Format :

SMTP uses RFC 822 standard for text message format:

header lines: describes the following information related with mail like,



(d) SMTP Architectures :

i) First Scenario :

- The sender and receiver of the email are users on the same mail server
- They are directly connected to shared mail server i.e. Both the sender and receiver are having the same mailbox on the same system.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

ii) Second Scenario :

- The sender and receiver of the email are users on two different mail servers.
- The message is need to be send over internet on the individuals Mailbox.

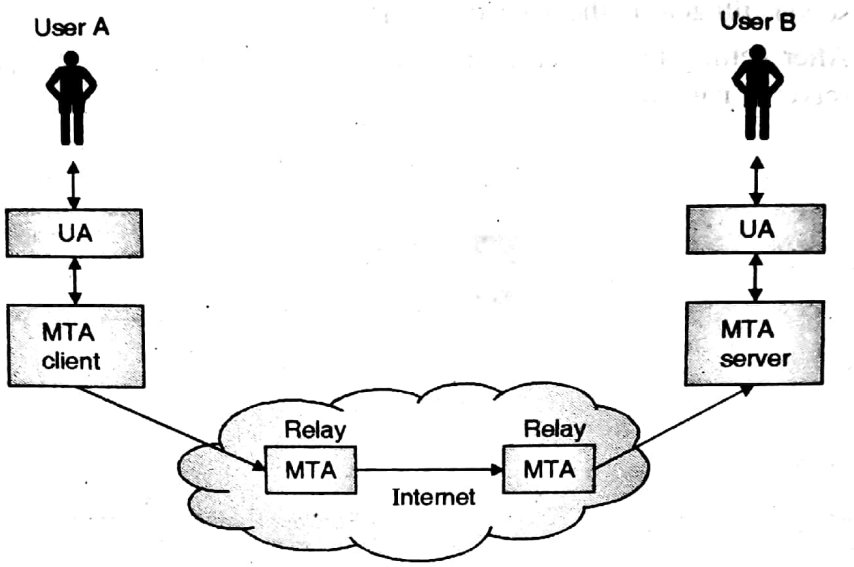


Fig. 7.2.4

iii) Third Scenario :

- One user is directly connected to mail server and the other one is separated from mail server and connected vis LAN / WAN.

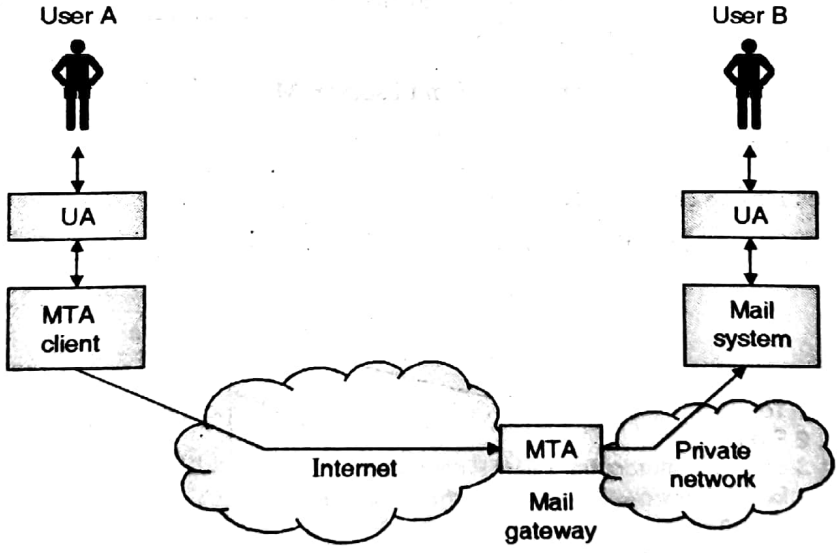


Fig. 7.2.5

iv) Fourth Scenario :

- Both the Sender and receiver are separated from mail server and connected via LAN/VAN

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(e) Working :

- At the Client side; SMTP Client sends mail to the SMTP Server's mail box
- Then the mail is transferred over the internet to found the required Destination's mailbox.
- The mail reaches to required destination.
- The mail is kept at server side SMTP server's mail box.
- Then through the mail access protocol the mail is transferred in the respective servers SMTP Client mail box.

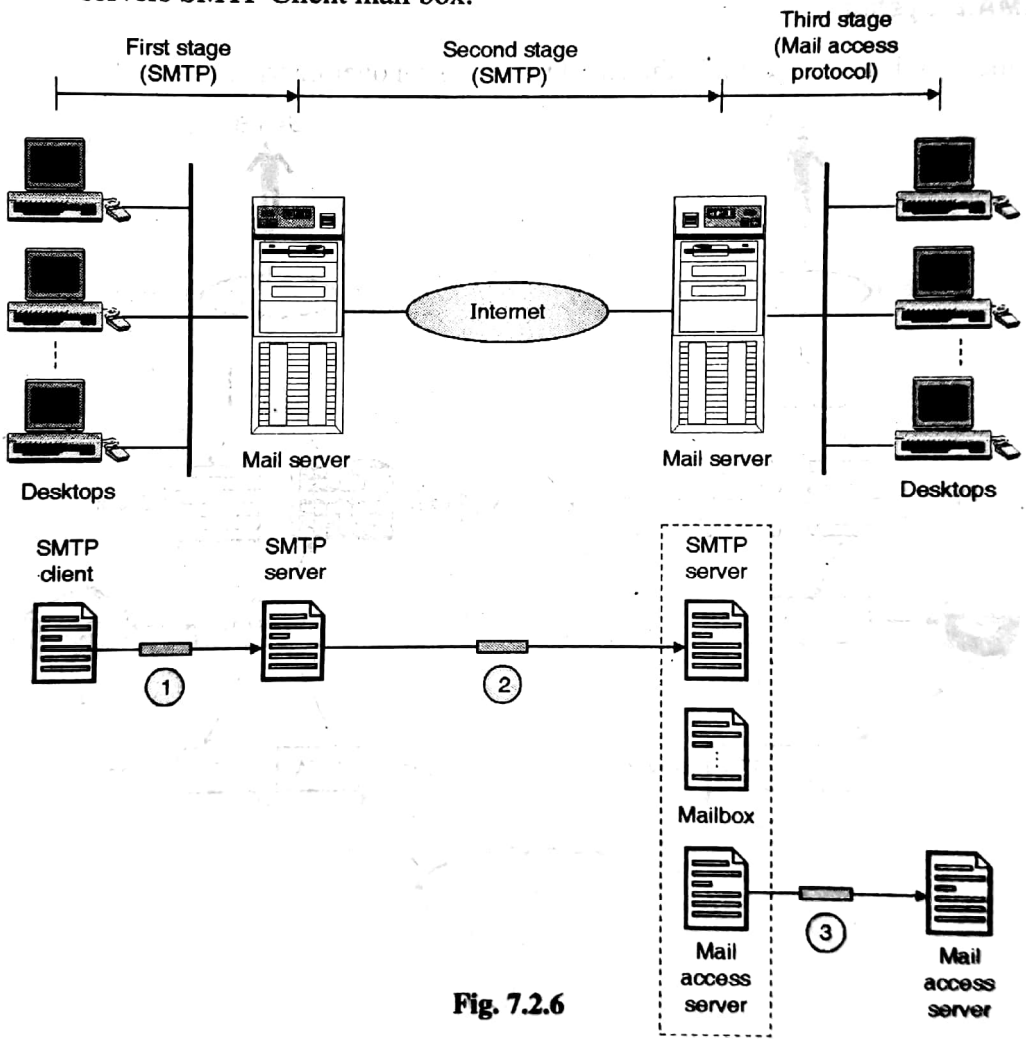


Fig. 7.2.6

(f) Address Format :

To send any message; receivers address as well as to know who is sender we need to specify the respective address of client and server.

The message format is as shown in the Fig. 7.2.7;

- First part contains the name of a client/server mail box on its local site.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Second part specifies domain name of destination.

For example xyz@gmail.com

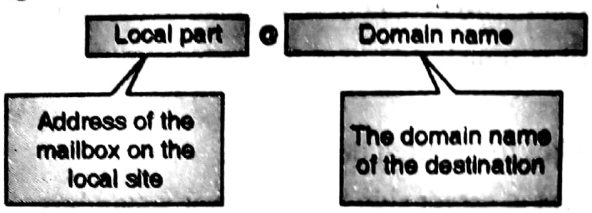


Fig. 7.2.7

(g) EMAIL System :

Following Fig. 7.2.8 explain the email transmission over internet :

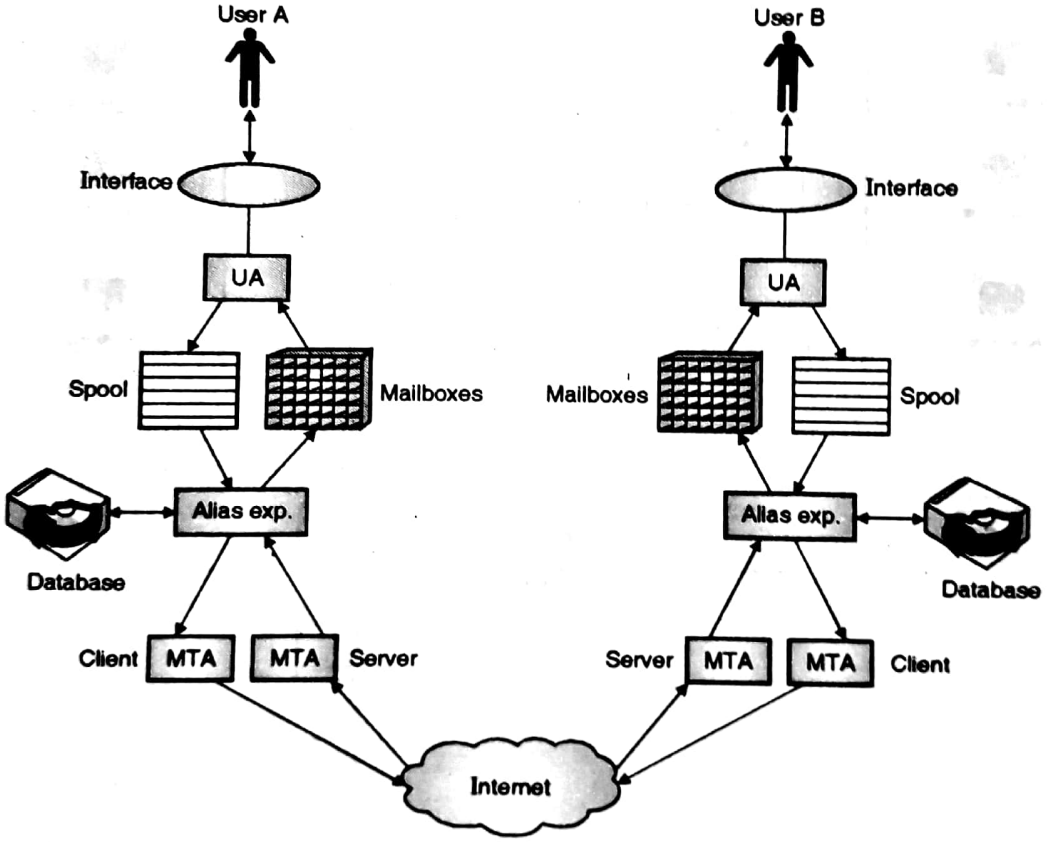


Fig. 7.2.8

- Client i.e. *User A generates* mail into its Spool by using interface through User Agent.
- Then the *Client Mail Transfer Agent* transfer it over the internet.
- The *server Mail Transfer Agent* receives the mail and saves it into the Server's mailbox.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Then Server i.e. User B able to read the mails from its own mail box through User Agent over the communication channel using interface.
- And same process steps are followed when User B wants to send mail to User A.

(h) Connections in SMTP :

Three major steps of SMTP connection between Client and Server are :

1. Connection Establishment
2. Message Transfer
3. Connection Termination

1. Connection Establishment :

As shown in the Fig. 7.2.9 the MTA Server sends *ready* message to MTA Client

- If MTA Client wants to accepts this message then replies with *HELO* message
- Then MTA Server gives response by sending *OK* message

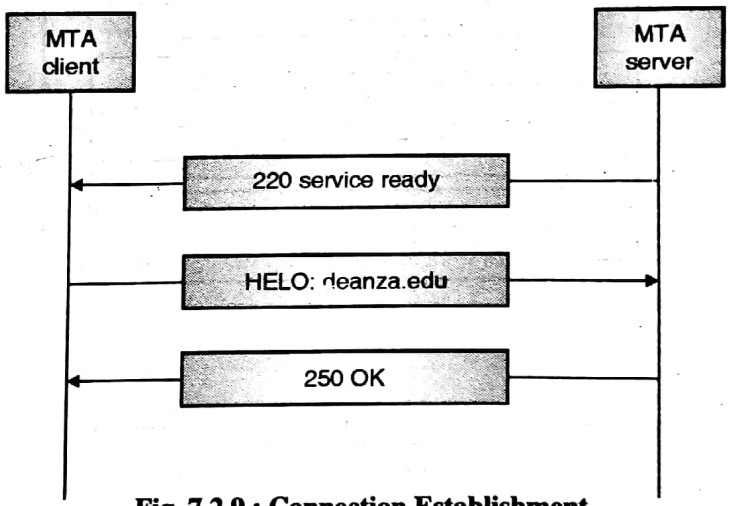


Fig. 7.2.9 : Connection Establishment

2. Message Transfer :

- After connection establishment between MTA Client and MTA Server the message transfer takes place with the help of SMTP commands and responses.
- Example of message transfer is as follows :
- As per the Fig. 7.2.10 message is transfer using three main parts:

(i) **Envelope :** It specifies the sender and receiver of a mail; whether the connection between them possible or not.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(ii) **Header :** It specifies the sender and receiver of a mail along with extra information like Date etc.

(iii) **Body :** It specifies the core information content of a mail i.e. the data part of message.

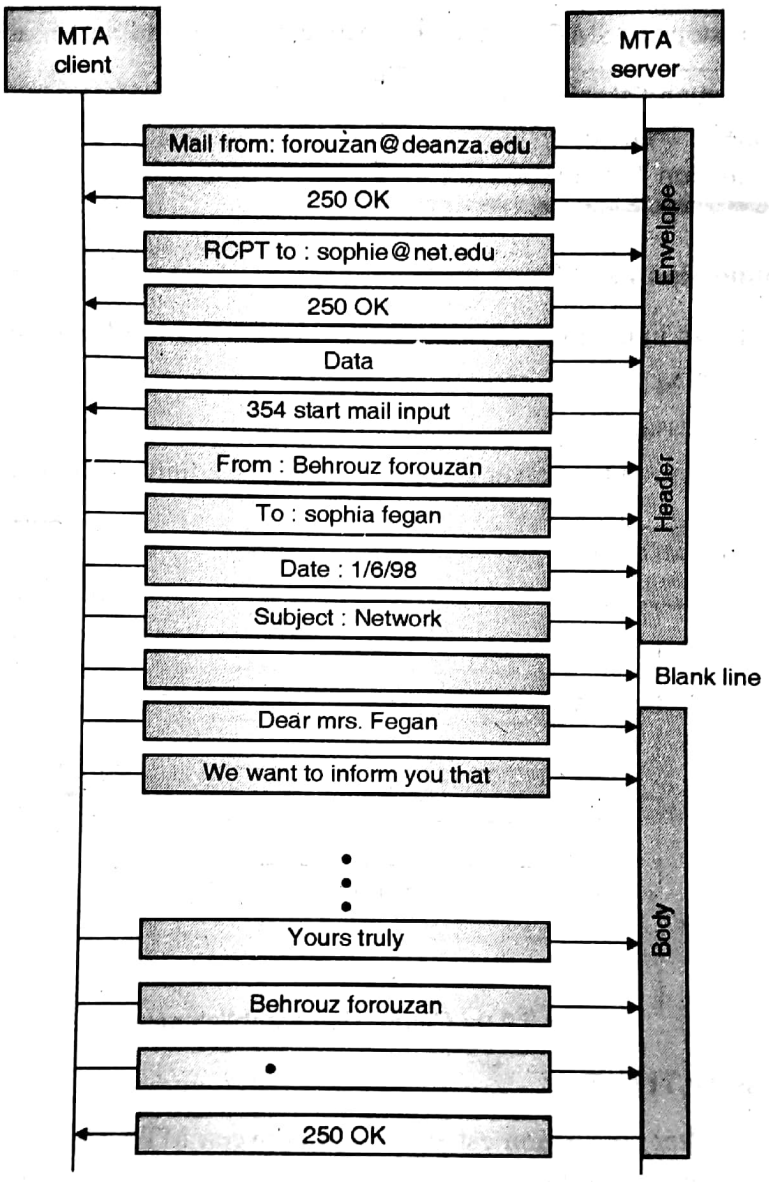


Fig. 7.2.10 : Message Transfer

3. Connection Termination :

- After the successful transfer of message MTA Client sends *Quit* message to MTA Server.
- Then MTA Server replies with response that *Service is closed.*

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

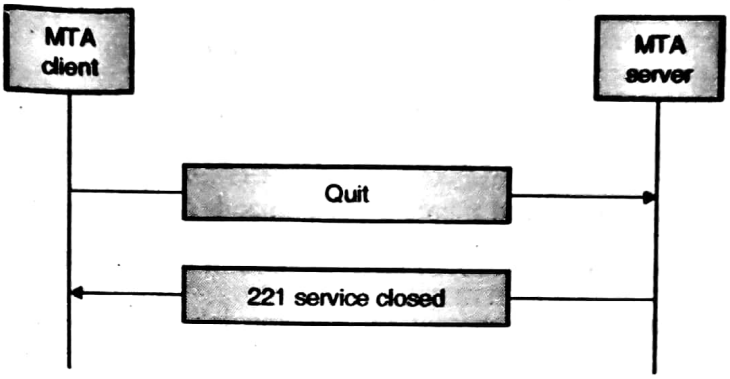


Fig. 7.2.11 : Connection Termination

(i) Commands and Responses :

- As we have discussed earlier SMTP is command-Response model between Client and Server.
- The commands are given by client to server and the response related with that commands are passed from server to client.

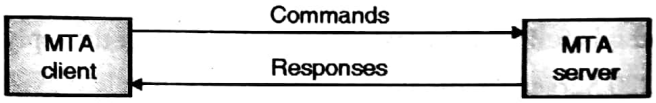


Fig. 7.2.12 : Commands and Responses

1. Command Format

Keyword : argument (S)

Some commands and their functions in the SMTP are listed down:

SMTP command	Command function
HELO	The command sent by a client to identify itself, with a domain name.
MAIL FROM	Used in the form MAIL FROM: to identifies the sender of the message.
RCPT TO	Used in the form RCPT TO: to identifies the message recipients.
TURN	It allows to perform reverse operation i.e. the client and server to switch their roles and send mail in the reverse direction without establish a new connection.
ATRN	The ATRN (Authenticated TURN) command optionally considers one or more domains as a parameter. The ATRN command not considered if the unauthenticated session is considered.
SIZE	Indicates the maximum message size supported by the SMTP server. The message should not be send by the clients that are larger than the size indicated by the server.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

SMTP command	Command function
ETRN	It is an extension of SMTP.SMTP server sends request to another server that "send any e-mail messages that it has" using this command.
PIPELINING	It helps to send a stream of commands dose not wait for response.
DATA	To initiate transfer of message content through client.
DSN	An ESMTP command for enabling delivery status notifications.
RSET	Resets the buffer and clear the entire message transferred till that time.
VRFY	Helps to verifies that a mailbox of particular receiver is available for message delivery
HELP	list of commands that are supported by the SMTP service are given by this command
QUIT	Helpful for termination of the session.

The command and response are forwarded between client and server in the form of a three digit number and it is followed by text which explain about the reply from the server.

For example : 220 Server Ready

500 Syntax error, command unrecognized.

The list of reply codes are shown below:

Most of them will not occur if mail server programmed correctly.

211	Indicates a system status or help reply.
214	Describes the help Message.
220	Indicates that server is ready.
221	Shows that server is ending the conversation.
250	Indicates that the requested action was completed.
251	The server will forward the mail message but the specified receiver is not local.
354	It indicates that sender can start sending the main part of message.
421	Save the mail messages and then the mail server will be shut down.
450	The mailbox is busy wait and try again.
451	Error occurred : The requested action not completed.
452	Mail server ran out : The requested action not completed due to the lack of system storage.
500	Syntax error/ Long sentence: The last command not completed .
501	Syntax error: parameters or arguments not ale to proceed.
502	The mail server not implemented the last command given by client.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

503	Last command given by client was out of sequence.
504	The parameters of the last command not implemented by the server given by client.
550	Mailbox not found or not having access rights of particular mailbox.
551	Forwarding address: The specified user is not local; hence message will contain a receivers address.
553	Syntactical error : The specified mail address not syntactically correct.
554	The mail transaction has failed due to unknown causes.

7.3 POP 3

Q. Write a note on POP3. MU - April 2013

1. Introduction :

- **Post Office Protocol3 (POP3)** is other mail access protocol which is widely used.
- POP just shows you what is in your inbox on the Users mail server, it checks the server for new messages, downloads all the new messages in your inbox onto your computer, and then deletes them from the server.

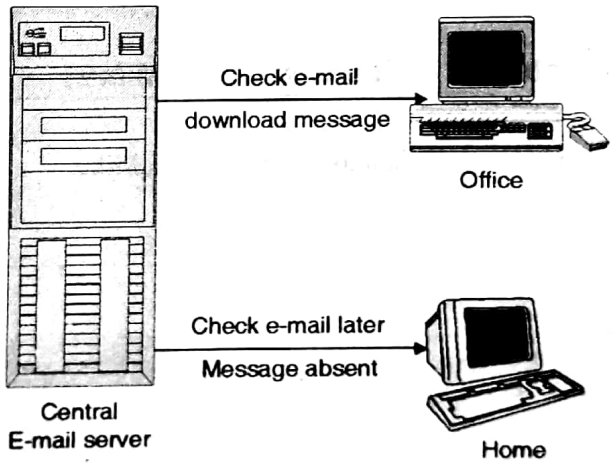


Fig. 7.3.1 : Post Office Protocol (POP)

2. Working :

- The working of POP3 is as shown in the Fig. 7.3.2,
- The POP3 Client first log in to the POP3 server using user name and password
- After the successful reply from server side client ask for the detail information about his mail box on server.
- Server displays the list of emails along with other required information.
- Then client starts retrieving/reading the emails from the server's mail box.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

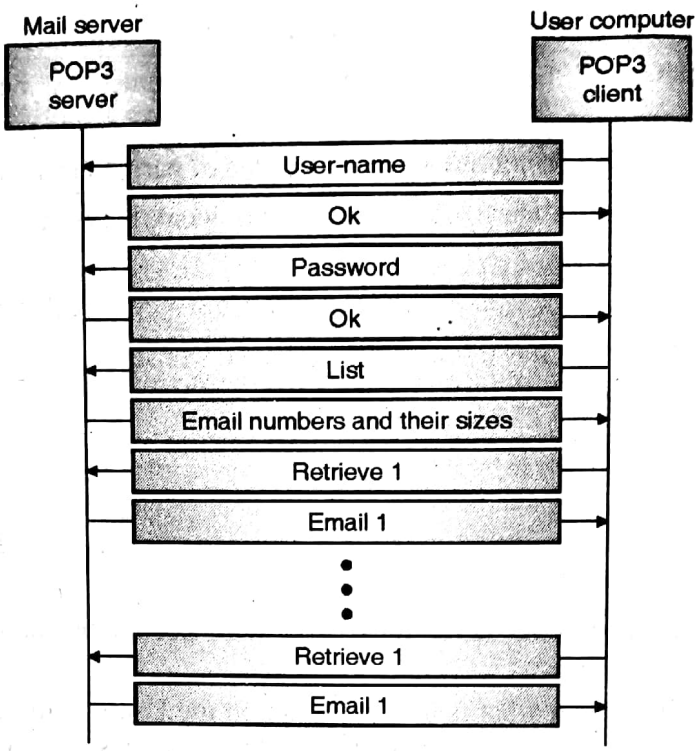


Fig. 7.3.2

7.4 Multi-purpose Internet Mail Extensions (MIME)

MIME helps to add non textual data to be sent in email like,

- Graphics image
- Voice files
- Video clips etc.

It also work in Client-Server model.

Sender :

- It encodes binary item into printable characters
- It helps to add printable characters in email message for transfer

Receiver :

- It receives email message containing encoded item
- After receiving the encoded mail it decodes message to extract original binary value.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

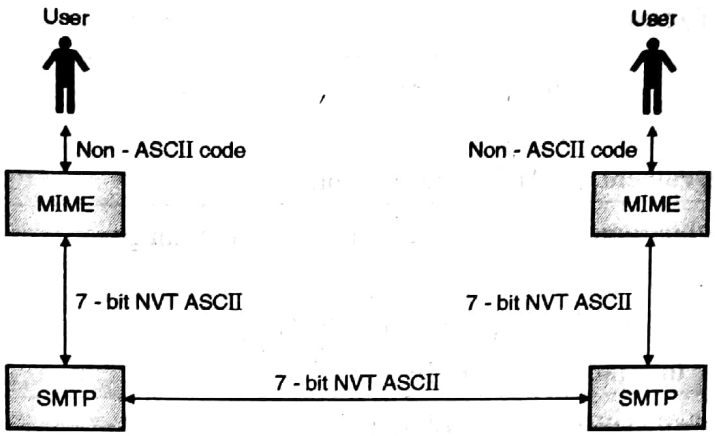


Fig. 7.4.1

As shown in the figure users i.e. Client / Server able to ad non ASCII code like Graphics in the mail using MIME ; which converts that data in ASCII code and easily transferable using SMTP over the internet.

(a) Message Format :

Email header	
MIME Version : 1.1	
Content-Type : type/subtype	
Content –Transfer-Encoding : encoding type	MIME header
Content-Id: message id	
Content-Description : textual explanation of non-textual contents	
Email body	

(b) Header :

Q. What are the different kinds of headers available in MIME? MU - April 2013

Email header :

It contains data about sender and receivers address along with the specification of subject.

MIME header :

Header in email message describes

Version :

It specifies the version used of MIME.

Content type along with sub type :

It specifies the type of data used in the main information. Content type and sub types are separated by the " / " (slash)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Seven Basic MIME Types :

Text	Describes Textual format for example a document. It has two main sub types : Plain document and HTML document.
Image	A still photograph or computer-generated static image. The subtypes are : Joint Photographic Experts Group (JPEG) Graphic Interface Format (GIF) etc
Audio	A message is in sound recording format. The subtype is Standard 8khz audio data.
video	Explain a video recording that includes motion. Time varying information i.e. animated data also displayed using this format. The subtype is Moving Picture Experts Group (MPEG)
application	Gives raw data for a program
multi-part	Contents Multiple messages that each have a separate content type and encoding It has subtypes : Mixed- the body of message contains ordered parts of various data types Parallel-the body of message contains unordered parts of various data types Alternative – It contains parts of versions of same message. Digest – Similar to mixed but default part is message.
message	It specifies an entire e-mail i.e. main body/ information about the subject and the connections with other necessary data.

encoding used :

It explain about which type of encoding techniques are used

Message ID :

It specifies a particular number for identification of a mail and it is used in every fragment of message.

Content explanation :

It gives description about the content in the body of a message.

Example :

Email Header : From : abc@acollege.ac.in
To: xyz@example.edu
MIME Header : MIME-Version: 1.0
Content-Type : image/jpeg
Content-Transfer-Encoding : base64

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Body :

The body contains the main information/data from the mail/message.

7.5 IMAP

- For retrieving the e-mail programs or messages from various systems over the network we are able to use two mail access protocols:
- Internet Message Access Protocol (IMAP) or Post Office Protocol (POP) .
- In a POP, client system stores e-mail messages in user's mailboxes on users system and keeps record of operations on messages like user have been read, replied to etc.
- POP client able to delete old messages from the server's system without users permissions.

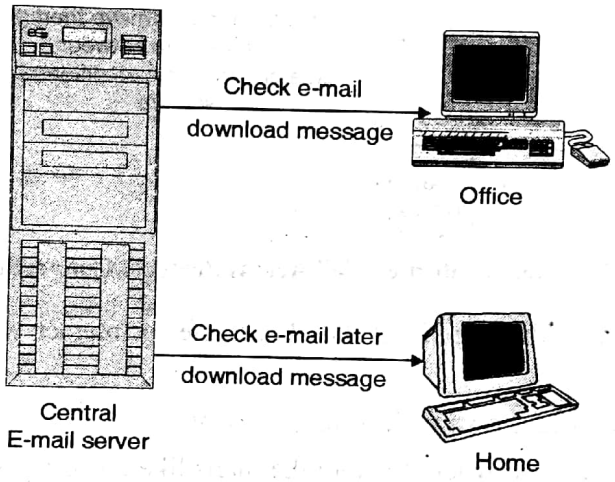


Fig. 7.5.1 : Internet Mail Access Protocol

- In the IMAP e-mail account, the original messages will remain on the server, along with operations performed on it like user read, replied to, or forwarded a message.
- IMAP stores folder structure in a main folder called "imap.hyperoffice.com".

(a) Introduction :

- Internet Mail Access Protocol is known as email access protocol of an application Layer.
- It helps client to access an e-mail from remote mail server.
- IMAP is useful to access messages from more than one computer in the network.
- IMAP protocol based on a TCP connection and works on default port 143.
- IMAP supports both on-line and off-line modes of operation.
- IMAP generally leave messages on the server until the user commands for deleting them.
- It support for concurrent access to shared mailboxes in the network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- It is not necessary that; client should know the details about server's file format.

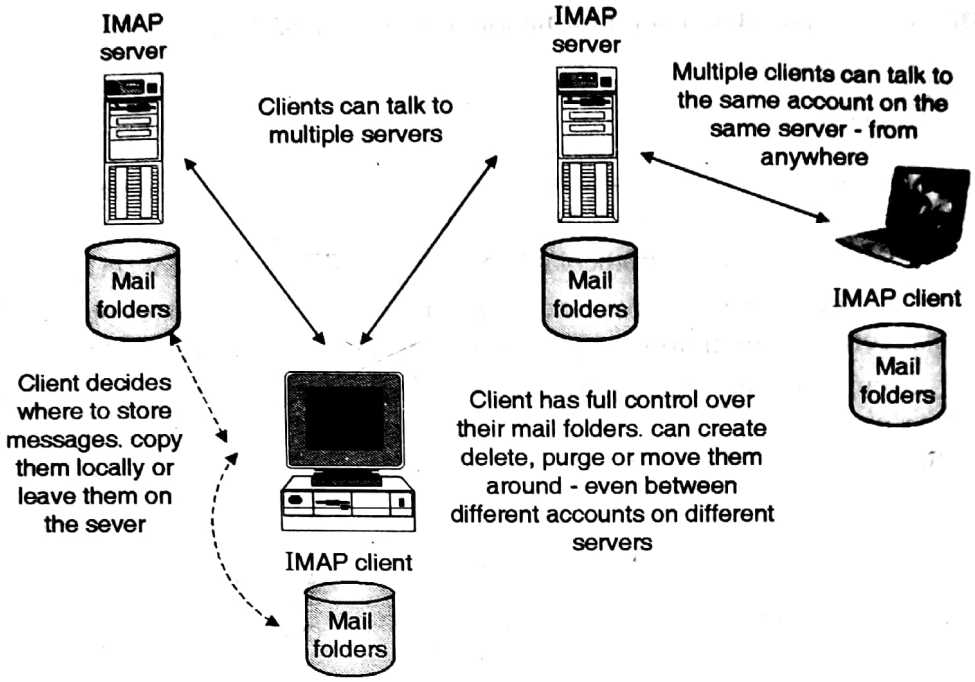


Fig. 7.5.2 : Internet Mail Access Protocol Connection

- As shown in the Fig. 7.5.2 the client able to interact with many servers at the same time.
- Client can access own mail from anywhere.
- Client can decide where to store the mails like on server's mail folder or on local mail folders.
- The mails are not deleted until client explicitly deletes them.

(b) Procedure of the IMAP protocol :

In IMAP all emails are kept on a mail server

Functionality :

1. IMAP Server's directory is considered as local directory hence work directly on server.
2. It performs operations on different folders like copy, delete, modify etc.
3. Using IMAP users are able to download message headers and later on the full messages.
4. IMAP's communication procedure :
   - Connection initialization
   - Interaction between client and server
   - Connection termination

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(c) Interaction between client and server :

- Client sends data and server receives.
- The Client-command begins with alphanumeric string called as "tag".
- For example "A001" is generated for every new command then the command with corresponding arguments followed.
  - (i) Server sends data and client receives.
  - (ii) Server receives and works with the command given by client.
  - (iii) Server response with the same tag with a state like "OK/NO/BAD".
  - (iv) The additional information begin with '*' called as untagged.
  - (iv) Untagged information can be sent at any time between client and server.

(d) Different states of an IMAP session :

Most commands of IMAP are only valid in special states otherwise: *protocol error*

States are :

1. **Initialization :** In this state the session using IMAP Server and IMAP Client is started.
2. **Non-Authenticated :** After connecting with IMAP server If Client's Status is Unauthenticated then the Client's session is terminated and Logout state takes place.
3. **Authenticated :** If the client is already having authentication then Client will Login and starts the session with IMAP Server.
4. **Selected :** After the session has started the Client will work on the selected data as per the requirement.
5. **Logout, Closed :** At the end after the completion of work the termination of connection takes place i.e. the Logout state.

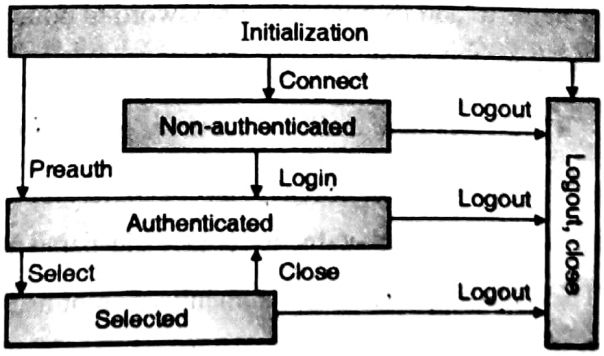


Fig. 7.5.3 : State diagram of IMAP

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

(e) Flags message attributes :

1. It consists of the list of token related with the message and sent by the server
2. A flag indicates permanent or session-only

System flag

(i) This flag name is predefined in the IMAP specification

(ii) All system flags are begin with '\'

Keywords

(i) A keyword in the IMAP message is defined by the server implementation

(ii) The keywords in IMAP dose not begin with '\'

Some System Flags are listed below :

- \Seen - indicates that Message has been read
- \Answered - indicates that Message has been answered
- \Flagged - informs that message is "flagged" for attention
- \Deleted - informs that message is "deleted" for removal by later EXPUNGE
- \Draft - describes that message has not completed composition and it is marked as a draft
- \Recent - It explain that message is "recently" arrived in this mailbox.

(f) Commands :

- LOGIN – It helps to add username and password to do login.
- SELECT – It indicates mailbox-name.
- CREATE – It indicates new-mailbox-name for generation.
- DELETE – It describes mailbox-name to delete.
- RENAME – It indicates new-name to replace old-name of mailbox.
- AUTHENTICATE – It is useful for authentication of users mailbox
- CLOSE – It indicates that the mailbox is closed.
- SEARCH – It denote the mailbox-name which user want to search.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- COPY – It indicates the mailbox-name from which user wants to copy some data

(g) Login :

We login using user's account and password, not "abc" and "xyz"!

- INPUT: a01 login abc xyz
- RESPONSE: a01 OK User logged in

(h) Logout :

Just by typing following statements we are able to do the Logout;

- a07logout
- * BYE LOGOUT received
- a07 OK Completed

(i) Advantages over POP :

- IMAP works in connected and disconnected modes of operation i. e. in online and offline modes of operations.
- Header-helps to do message retrieval
- Multiple clients at the same instance connected to the same mailbox using IMAP.
- IMAP helps to provide message state information
- There exists multiple mailboxes on the IMAP server
- IMAP helps to provide Server-side searches facility.
- IMAP can create e-mail folders on the server; these folders are accessible from anywhere. If POP is used and create e-mail folders, they are stored locally then user cannot access these folders from anywhere except the computer on which user created them.

7.6 Multimedia

1. Introduction :

- Multimedia is now a days very popular on internet for advertising, entertainment and to access various information from world.
- People access internet not only for text but for audio video search as well.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

2. Multimedia Services :

The audio video services on internet are generally divided in three categories.

a) Streaming Stored Multimedia :

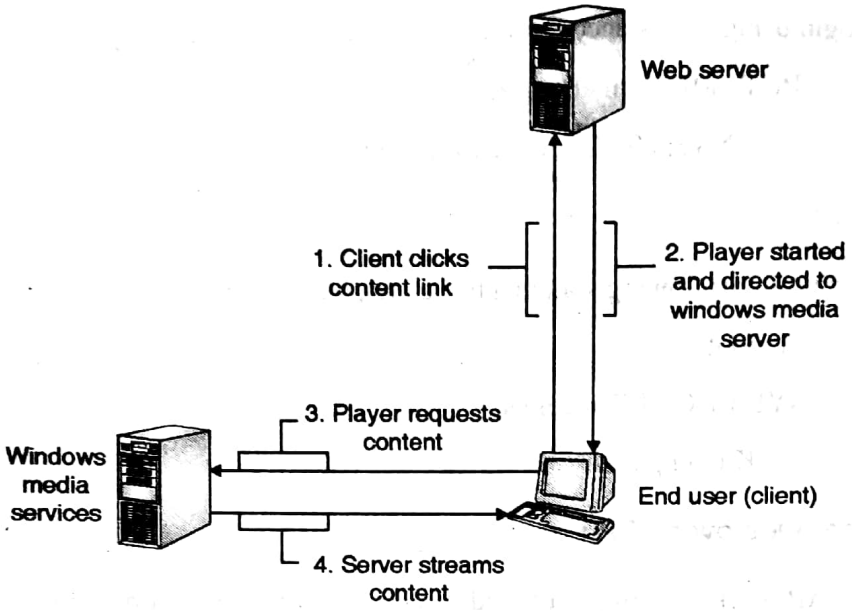


Fig. 7.6.1

- **Introduction :**
  - Multimedia file are compressed and then stored on to multimedia server.
  - These file can be accessed by various internet users by downloading it from the network.
  - In this type of multimedia user accesses the broadcasted audio and video from online broadcast server.

- **Working :**
  - End user sends GET request to server machine to which web server sends response.
  - Then audio file can be played by using media player services.
- **Example :**
  - On demand audio video
  - Live Cricket matches broadcasted on internet

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

b) Streaming Live Multimedia :

- **Introduction :**
  - In this type of multimedia user accesses the broadcasted audio and video from online broadcast server.
- **Working :**

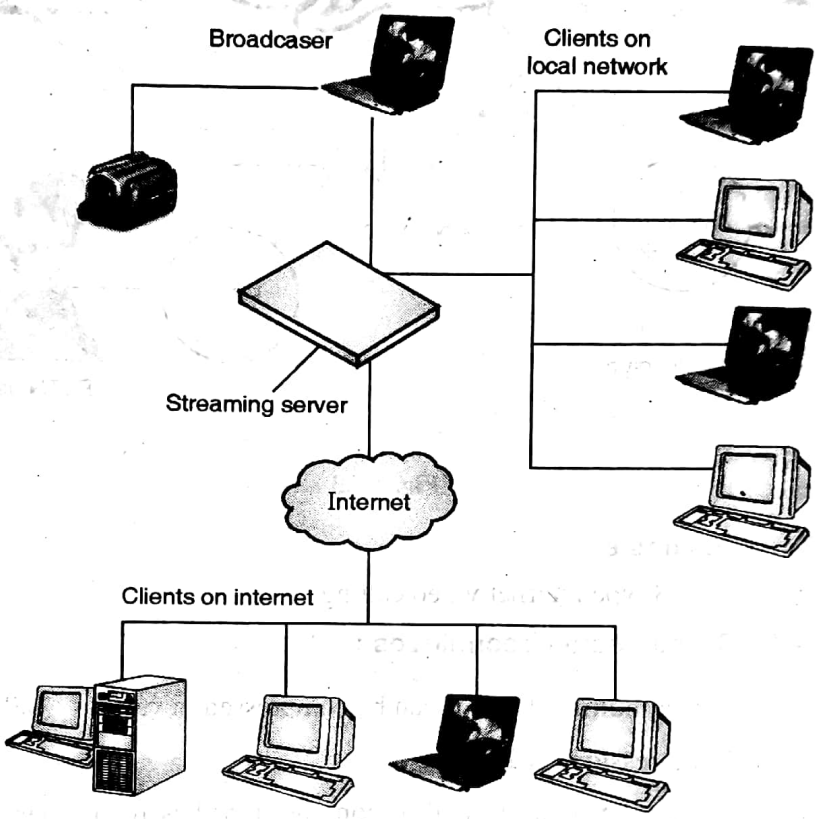


Fig. 7.6.2

- **Example :**
  - Live Cricket matches broadcasted on internet

c) Interactive Multimedia :

- **Introduction :**
  - Multimedia can be used to communicate with people over the world and attached by internet.
  - Only required multimedia file will be sent to receiver.
  - Works on basis of RTP (Real time audio video protocol)

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Working :**

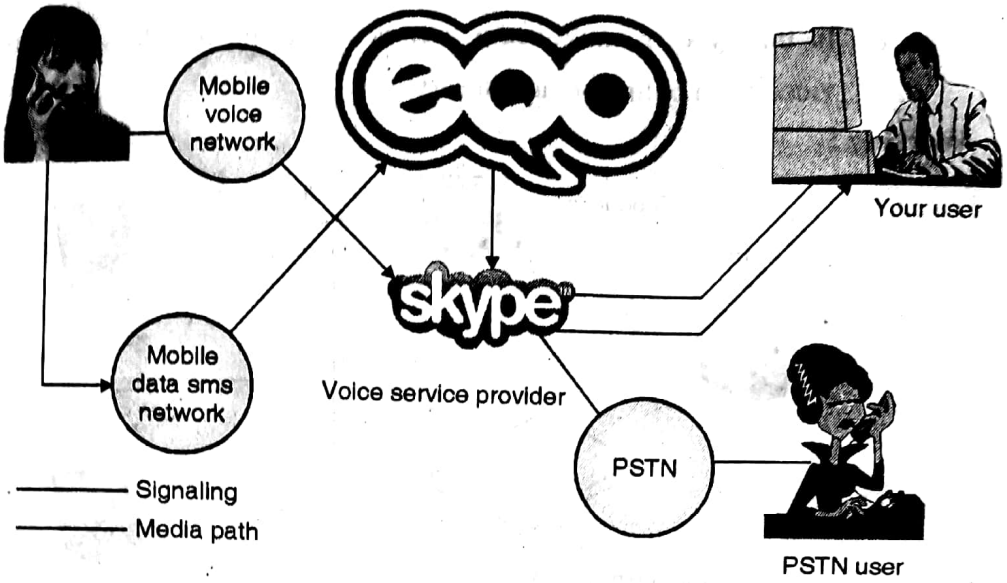


Fig. 7.6.3

- **Example**
  - Skype internet video calling

3. Multimedia Compression Techniques :

- The different multimedia files can be compressed in various available technique,
- Audio Compression : MP3
- To produce CD quality audio compression based on perceptual encoding technique we make use of MP3 coding.
- MP3 uses frequency and temporal masking for compressing audio signal.
- MP3 audio files can produces data rates 96 kbps,128 kbps and 160 kbps.
- It is a part of MPEG coding.

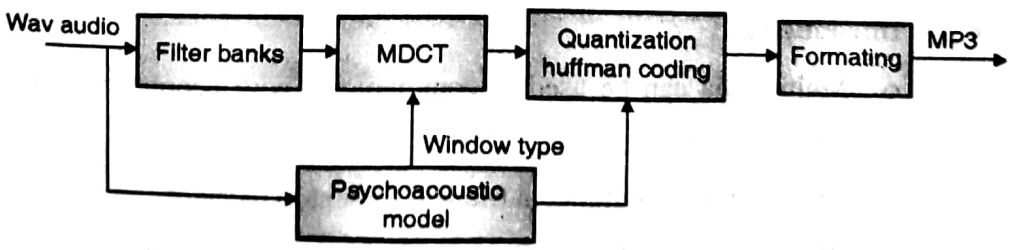


Fig. 7.6.4

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- Image Compression : JPEG
- JPEG is a common image format used in World Wide Web.
- JPEG compressed images can be used to hide data for secret internet communication.
- It makes use of DCT and binary coding.

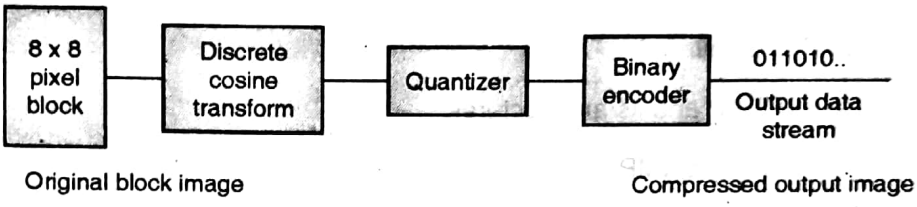


Fig. 7.6.5

- Video Compression : MPEG
- A compression encoder works by identifying the useful part of a signal which is called the entropy and sending this to the decoder.
- The remainder of the signal is called the redundancy because it can be worked out at the decoder from what is sent.
- In MPEG the two-dimensional spatial frequency analysis is performed using the Discrete Cosine Transform (DCT).
- An array of pixels, typically 8 x 8, is converted into an array of coefficients.
- The magnitude of each coefficient represents the amount of a particular spatial frequency which is present.

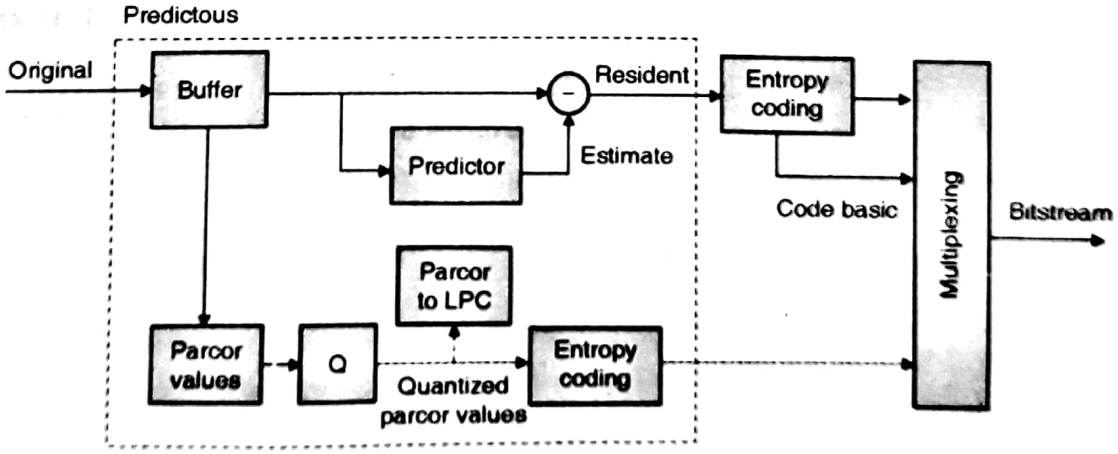


Fig. 7.6.6

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Review Questions

Q. 1 Write a short note on multimedia internet technologies.

Q. 2 Explain various multimedia compression techniques.

Q. 3 Describe multiple multimedia services in details.

Q. 4 Write a short note on application layer protocol.

Q. 5 Explain IMAP in detail.

Q. 6 Explain use of SMTP and its architectures.

Q. 7 Write a short note on SNMP.

Q. 8 Explain difference between SMTP POP3 and IMAP.

Q. 9 Explain connections in SMTP

Q. 10 Working of SMTP POP3 and IMAP.

7.7 University Questions and Answers

April 2013

Q. 1 Write a note on POP3. **(Section 7.3)** **(5 Marks)**

Q. 2 Explain the user agent component of electronic mail system. **(Sections 7.2 (a))** **(5 Marks)**

Q. 3 What are the different kinds of headers available in MIME? **(Section 7.4(b))** **(5 Marks)**

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Appendix A

List of Practical's

➢ **Practical 1 :** IPv4 Addressing and Subnetting

a. Given an IP address and network mask, determine other information about the IP address such as:

Network address

Network broadcast address

Total number of host bits

Number of hosts

b. Given an IP address, network mask and sub network mask, determine other information about the IP address such as:

The subnet address of this subnet

The broadcast address of this subnet

The range of host addresses for this subnet

The maximum number of subnets for this subnet mask

The number of hosts for each subnet

The number of subnet bits

The number of this subnet

Preferred Programming Tools

- **Environment** Windows or Linux or Unix

➢ **Practical 2 :** Use of ping and tracert / traceroute and arp utilities.

Preferred Programming Tools

- **Development Tool :** Java Development Kit 1.4 or above
- **Environment** : Windows or Linux
- **IDE** : Packet Tracer

➢ **Practical 3 :** Configure IP static routing..

Preferred Programming Tools

- **Development Tool :** Java Development Kit 1.4 or above
- **Environment** : Windows or Linux
- **IDE** : Packet Tracer

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Practical 4 :** Configure IP routing using RIP.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 5 :** Configuring OSPF.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 6 :** Configuring UDP and TCP.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 7 :** Run different STCP commands.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 8 :** Configure DHCP and DNS.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 9 :** Configure FTP and HTTP. Run Telnet and SSH.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

- **Practical 10 :** Configure SMTP, POP3, IMAP and MIME.

  Preferred Programming Tools

  - **Environment** : Windows or Linux
  - **IDE** : Packet Tracer

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Appendix

B

Client Server Socket Programming using JAVA

B.1 Sockets

1. Introduction

- A *socket* is fundamental technology of computer networking used to create a connection between two computers.
- Socket mechanism allows applications to communicate using standard mechanisms with help of network hardware and operating systems.
- The Sockets Application Program Interface (API) provides a library of functions which are used to develop network applications.
- Sockets are identified by Internet address, end-to-end protocol, and port number.
- A socket pair identifies all four components like source address and port number as well as destination address and port number.
- Sockets are acting like end point to communicate with each other.

2. Point to point communication

- A socket generally represented as a single connection between exactly two pieces of software or computers.
- Software based on sockets runs on two separate computers which are in the network.
- Sockets can also be used for inter process communication on a single computer.
- The Sockets are bidirectional that means any of two sockets is capable of both sending and receiving data.

3. Client

- A client is a system that accesses the remote service on another computer using network.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The application that initiates communication is generally called as client socket.

4. Server

- Server is a computer program that provides services to other computer programs in the same or other computers on network.
- The application that answers the client socket as generally called as server socket.

B.2 Socket Interface

1. Introduction

- The socket interface is made using kernel which contains 3 layers as below :
  - i. Socket layer
  - ii. Protocol layer
  - iii. Device layer.
- **Socket layer :** This interface is exists between the subroutines and lower layers
- **Protocol layer :** It will have the protocol used for communication
- **Device layer :** It has the device drivers which control the network devices.

2. Relationship

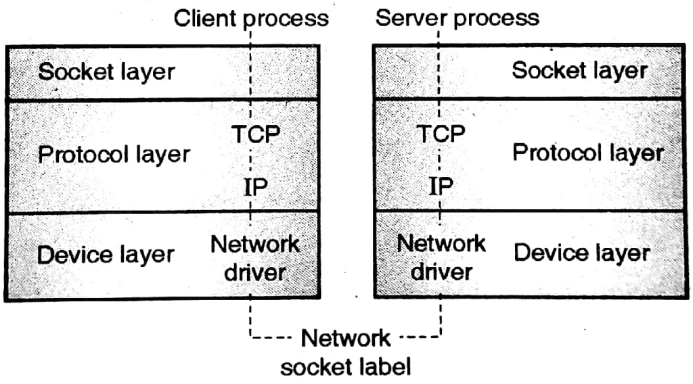


Fig. B.2.1 : Socket interface layers

- In above Fig. B.2.1 client process on the left with the socket layer under it and the protocol layer and device layer adjusted below it.
- The protocol layer lies between the other two layers.
- Corresponding layers are exists below the server process on the right.
- A line showing the network runs through all layers and connects the server with client processes (in above diagram U shape line).

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

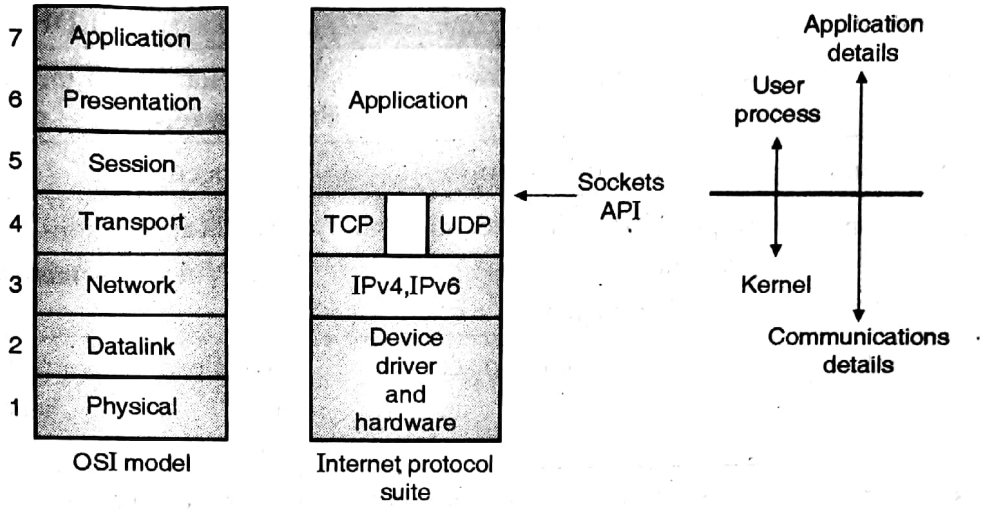


Fig. B.2.2

- The Internet does not follows entire OSI model but rather merges several of the protocols layers together.
- It is possible for two network applications to begin simultaneously, but generally it is not required hence we will do network operations in sequence, rather than simultaneously.
- The server executes first and waits to receive request from clients; the client afterwards and sends the first network packet to the server.

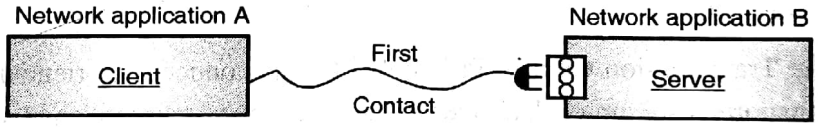


Fig. B.2.3

- After initial connection phase anyone the client or the server is capable of sending or receiving data.

B.3 Types of Socket

1. Datagram sockets

- The User Datagram Protocol (UDP) transports packets in a connectionless manner.
- In such communication, each data packet which is also called as a datagram is addressed and routed individually and may arrive at the receiver in random order.
- Datagram socket is designed to use with connectionless protocols.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Parameter	TCP	UDP
1. Reliability	Reliable communication	Unreliable still on time delivery of packets.
2. Connection	Connection-oriented	Connectionless
3. Applications	Applications that require safely guarantee. (eg. File transfer)	Media applications (eg. Voice transmissions.)
4. Flow control	Flow control and error-control	No flow or sequence control. User must handle these manually.
5. Socket type	Uses byte stream as unit of transfer. (Stream sockets)	Uses datagrams as unit of transfer. (datagram sockets)
6. Data exchange	Allows two-way data exchange (full-duplex)	One directional data transfer. (half-duplex)
7. Example	Telenet uses stream sockets. (everything you write on one side appears exact in same order on the other side)	TFTP (Trivial File Transfer Protocol) - uses datagram sockets.

2. Stream Socket

- The Transmission Control Protocol (TCP) is connection oriented protocol and it transports a stream of data over a logical connection established across the sender computer and the receiver computer.
- In such communication data sent from a sender is guaranteed to be received by recipient in the order it is sent from sender.
- Stream sockets are designed to use with connection oriented protocols.

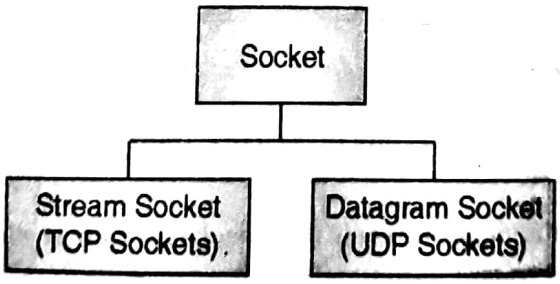


Fig. B.3.1 : Socket Types

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3. Raw Socket

- Sometime protocols like ICMP and OSPF uses services direct from IP.
- Raw sockets are designed for applications based on such protocols.

B.4 Ports

1. Introduction

- A port is a 16-bit number which is used by the host-to-host protocol to identify to which higher-level protocol or process it must deliver incoming messages coming from other host.
- Whenever any process wants to communicate with another process, it identifies itself to the TCP/IP protocol suite by one or more ports.
- Problem arises when different applications trying to use the same port numbers on one host is which should be avoided by writing applications to request an available port from TCP/IP.
- Because this port number is dynamically assigned, it may differ from one invocation of an application to the next.

2. Categories

- Port numbers are divided into three different categories as given below:
- Ports 0 through 1023
  - i. They are called as well known ports.
  - ii. They are associated with services in a static manner.
  - iii. E.g. HTTP servers would accept requests at port 80.
  - iv. The "well-known" ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) and most systems can only be used by system programs run by privileged users.
- Port numbers 1024 – 49151
  - i. They are called as registered port numbers.
  - ii. They generally used for multiple purposes.
  - iii. These port numbers are not controlled by the IANA and systems can be used by ordinary user-developed programs.
- Port 49152 – 65535
  - i. They are Dynamic and private port numbers
  - ii. No services associated with them.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Port	Service Name, Alias	Description
1	tcpmux	TCP port service multiplexer
7	echo	Echo server
9	discard	Like/dev/nu11
13	daytime	System's date/time
20	ftp.data	FTP data port
21	ftp	Main FTP connection
23	telnet	Telnet connection
25	smtp.mail	UNIX mail
37	time.timeserver	Time server
42	nameserver	Name resolution (DNS)
70	gopher	Text/menu information
79	Finger	Current users
80	www.http	web server

B.5 Socket Programming using Java

1. IPC

- Socket programming is used for implementing IPC (Interprocess communication) with java programming.
- IPC used for separate, independent processes to communicate among themselves to work together on any task.
- A process can be a sender of the communication or it can be a receiver of the data at another instant.

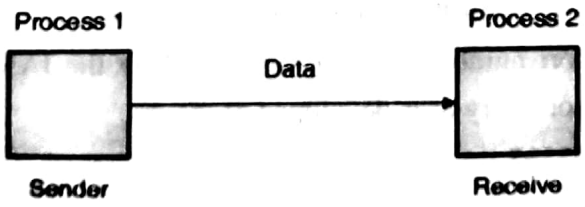


Fig. B.5.1 : Interprocess communication

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- **Unicast**

  In this transfer data is sent from one process to another single process.

- **Multicast**

  In this transfer data is sent from one process to more than one process at the same point of time.

- **Broadcast**

  In this transfer data is sent from one process to all other available processes at the same time.

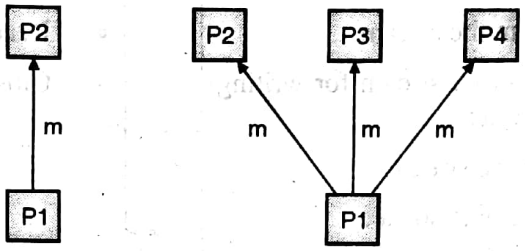


Fig. B.5.2

B.6 Connection Oriented (Stream Mode / TCP) socket

1. Introduction

- The Connection-Oriented Sockets are generally depends on the stream-mode I/O model of the LINIX Operating System that we have learn in last semester in which data is transferred with help of a continuous flow of data stream from a source to a destination.
- Data is added into the stream by a sender process which is also called as the server.
- Data is extracted from the stream with help of receiver process which is also called the client.

2. Working

- The server process first creates a connection socket and then listens for connection requests from other processes.
- Server will accept only one connection request at a time.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Connection Listener (Server)	Connection Requestor (Client)
• Create a connection socket • Listen for connection requests. • Accept a connection • Create a data socket • Get an input stream for reading to the socket • Read from the stream • Get an output stream for writing to the socket • Write to the stream • Close the data socket • Close the connection socket	• Create a data socket • Request a connection • Get an outputstream for writing to the socket • Write to the stream • Get an inputstream • Read from the stream • Close the data socket

- Whenever the connection request is accepted by server, a data socket is created with help of which the server process can write or read from or to the data stream.
- Socket is closed when the communication session between the two processes is over.
- The data and the server process is now free to accept another connection request.

3. Problems

- Server process is blocked when it is waiting for other incoming connection requests.
- This problem can be solved by spawning threads, one for each incoming client connection request and each thread will individually handle the particular client from a source to a destination.

4. Methods used in stream mode socket API

- The common key methods of the stream-mode socket API are explained as given below;
- These sockets are typically used for connection-oriented communication during which a sequence of bytes is transferred in one or both directions.
- The connection listener program (Server program) should be started before executing the client program.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sr. No.	Constructor/Method	Description
	ServerSocket class	
1.	ServerSocket(int port)	Create an object of class Server Socket and binds the object to the specified port.
2.	accept( )	This is a blocking method Call the server to listens or wait for any incoming client connection request When a client contacts it proceeds further then method is unblocked Returns a socket object to the server program to communicate with the client.
3.	Close ( )	Closes the ServerSocket object
4.	Void setSoTimeout (int timeout)	The ServerSocket object is set to listen for an incoming client request When the timeout expires, a java.net.SocketTimeoutException is raised. The timeout value must be > 0; a timeout value of 0 indicates infinite timeout.
	Socket class	
5.	Socket(InetAddress host, int port)	Creates a stream socket Connects it to be specified port number at the specified IP address
6.	InetAddress getInetAddress( )	Returns the IP address at the remote side of the socket
7.	InetAddress getLocalAddress( )	Returns the IP address of the local machine to which this socket is bounded
8.	Int getPort( )	Returns the port number of remote machine to which this socket in connected
9.	Int getLocalPort( )	Returns the local port number to which this socket is bound

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sr. No.	Constructor/Method	Description
10.	Inputstream getInputstream ( )	Returns an input stream for this socket to read data sent from the other end of the connection.
11.	OutputStream getOutputStream ( )	Returns an output stream for this socket to send data to the other end of the connection.
12.	Close( )	Closes this socket
13.	void setSoTimeout(int timeout)	Sets a timeout value to block on any read( ) call on the InputStream associated with this socket object. When the timeout expires, java.net.SocketTimeoutException is raised. The timeout value must be > 0; a timeout value of 0 indicates infinite timeout.

5. Simple TCP Server Programming

a) **Locate or find IP address and protocol number of server.**

b) **Open the Server Socket**

E.g.

```
ServerSocket connectionSocket = new ServerSocket(serverPortNumber);
```

c) **Wait and accept the Client Request**

Specify that the connection needs an arbitrary, unused port on local machine and allow TCP to select one

E.g.

```
Socket dataSocket = connectionSocket.accept();
```

d) **Create I/O streams for communicating to the client**

Specify the server to which messages is needs to be sent

E.g.

```
PrintStream socketOutput = new PrintStream(dataSocket.getOutputStream());
```

Or otherwise

```
DataInputStream is = new DataInputStream(dataSocket.getInputStream());
DataOutputStream os = new DataOutputStream(dataSocket.getOutputStream());
```

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

e) **Perform communication with client using application-level protocol**

E.g.

socketOutput.println(message);

Or otherwise

To Receive from client: String line = is.readLine();

For Sending to client: os.writeBytes("Hello Client");

f) **Close the socket**

E.g.

connectionSocket.close( );

6. Simple TCP Client Programming

a) **Locate or find IP address and protocol number of server.**

b) **Create a Socket Object**

E.g.

Socket clientSocket = new Socket(acceptorHost, serverPortNum);

c) **Create I/O streams for communicating with the server**

E.g.

BufferedReader br =

new BufferedReader(new InputStreamReader(clientSocket.getInputStream()));

Or otherwise

is = new DataInputStream(clientSocket.getInputStream());

os = new DataOutputStream(clientSocket.getOutputStream());

d) **Perform communication with the server**

Specify the server to which messages is needs to be sent

E.g.

System.out.println(br.readLine());

Or otherwise

Receive data from the server: String line = is.readLine();

Send data to the server: os.writeBytes("Hello Server..");

e) **Close the socket**

E.g.

clientSocket.close( );

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

➢ **Program 1 : Socket program to send sample message from server to client when it connects to server using TCP.**

Code for Server:

```
import java.net.*;
import java.io.*;
class TCP_Server
{
public static void main(String[] args)
{
try{
    System.out.println("-----------------------------------------");
    System.out.println("Program : TCP Server Socket");
    System.out.println("-----------------------------------------");
    String message = args[0];
    int serverPortNumber = Integer.parseInt(args[1]);
    ServerSocket connectionSocket = new ServerSocket(serverPortNumber);
    Socket dataSocket = connectionSocket.accept();
    PrintStream socketOutput = new PrintStream(dataSocket.getOutputStream());
    socketOutput.println(message);
    socketOutput.flush( );
    dataSocket.close( );
    connectionSocket.close( );
}
catch(Exception e){e.printStackTrace();}
    System.out.println("Message sent to client...");
    System.out.println("-----------------------------------------");
}
}
```

Code for Client

```
import java.io.*;
import java.net.*;
class TCP_Client
```

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study


```
{
public static void main(String[] args)
{
try{
    System.out.println("----------------------------------------");
    System.out.println("Program : TCP Client Socket");
    System.out.println("----------------------------------------");
    System.out.print("Message From Server is: ");

InetAddress acceptorHost = InetAddress.getByName("localhost");
int serverPortNum = Integer.parseInt(args[0]);
Socket clientSocket = new Socket(acceptorHost, serverPortNum);
BufferedReader br = new BufferedReader(new
InputStreamReader(clientSocket.getInputStream()));
System.out.println(br.readLine());
System.out.println("----------------------------------------");
clientSocket.close();
}
catch(Exception e){e.printStackTrace();}
}
}
```

Running above code :

Step 1: Compile and run server socket

Copy java code file to bin folder of java

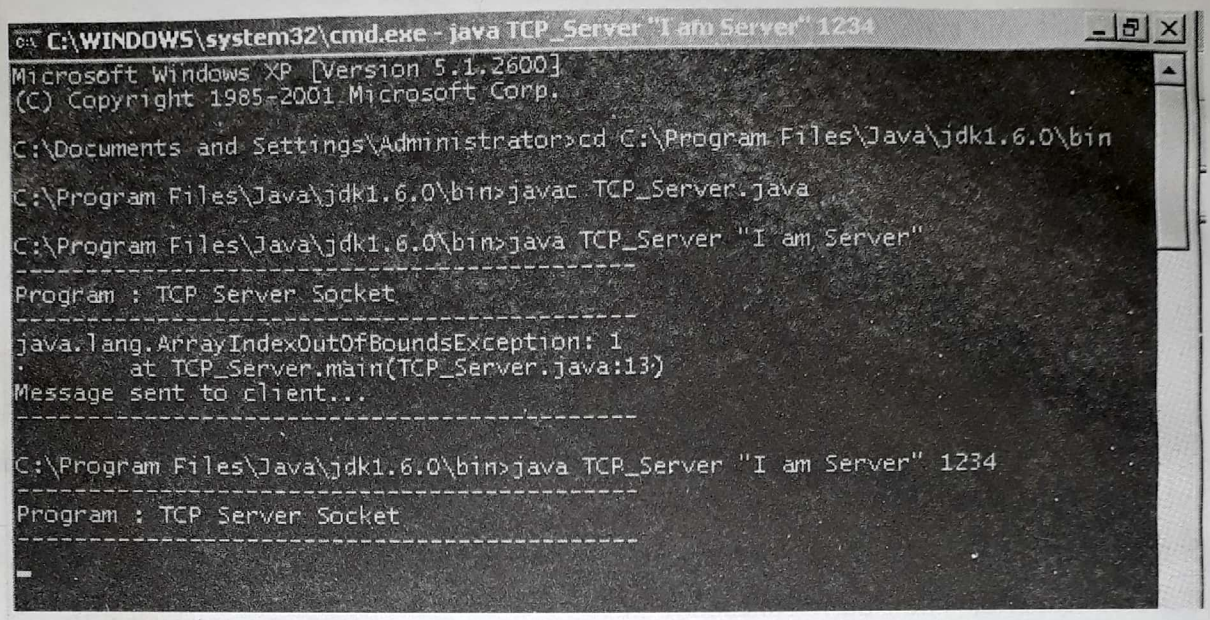
Compile TCP_Server.java program using javac command

Run TCP_Server.java program using java command pass port number as argument in below program 1234 is port number.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Output :



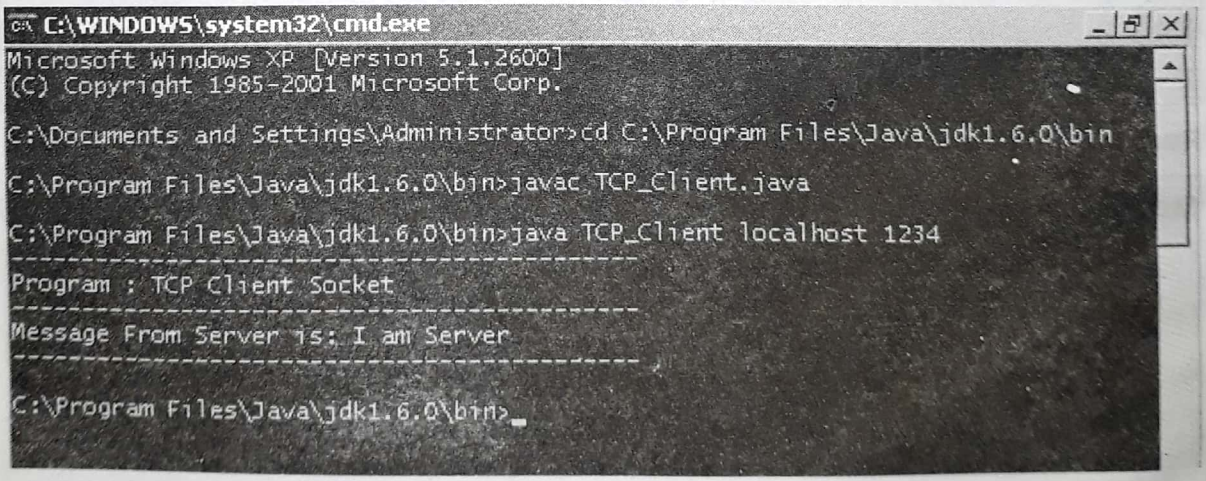
Step 2: Compile and run Client socket

Copy java code file to bin folder of java

Compile TCP_Client.java program using javac command

Run TCP_Client.java program using java command pass port number as argument in below program 1234 is port number.

Output

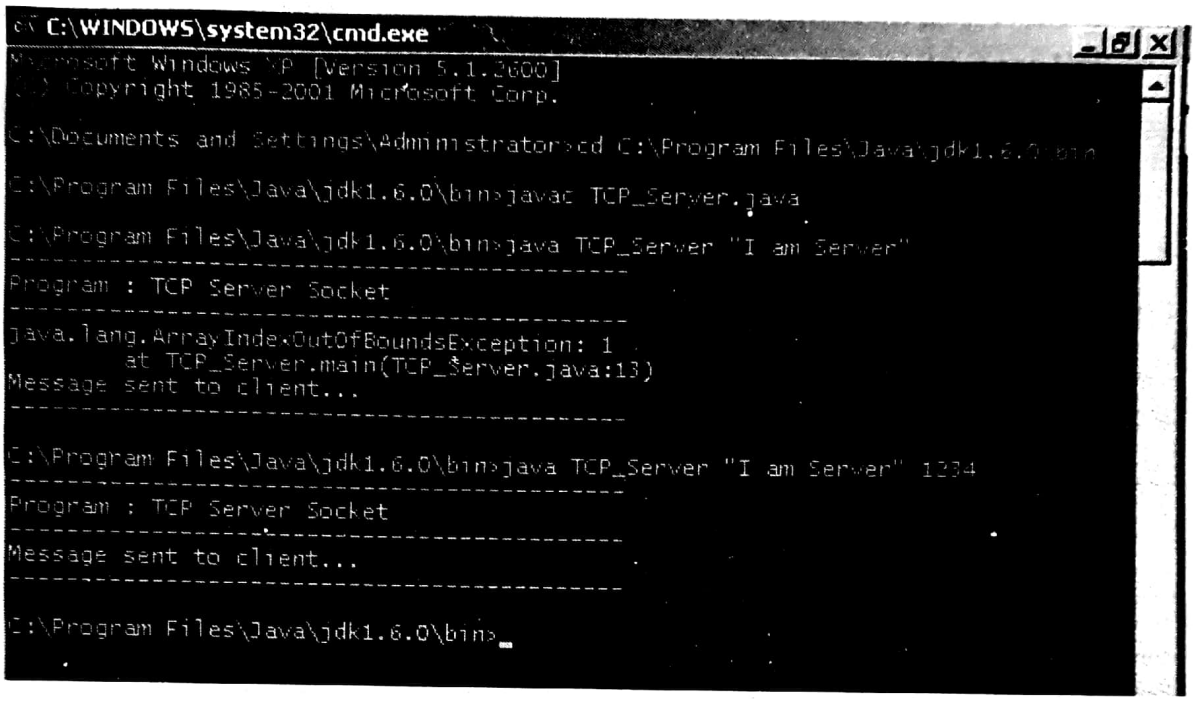


www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Step 3: Server socket Status after sending message to client

Output :



B.7 Connectionless (Datagram / UDP) Socket

1. Introduction

- In case of connectionless socket we use the datagram socket for delivery of datagram packets.
- UDP is unreliable and does not guarantee the delivery of packets in same order as they sent from server.
- Java have two classes for the datagram socket API:
  - (a) The DatagramSocket class : Used for the sockets
  - (b) The DatagramPacket class : Used for the packets exchange

2. Working

- Any process that wishes to send or receive data using the datagram socket API must instantiate a DatagramSocket object, which will be bound to a UDP port of the machine and it is local to the process.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sender Program	Receiver Program
Create a DatagramSocket object	Create a datagramSocket object
Bind it to any local port	Bind it to a specific local port
Place the data to send in a byte array	Create a byte array for receiving the data
Create Datagrampacket object, specifying the data array and the receiver's address	Create a DatagramPacket object
Invoke the send method of the DatagramSocket object and pass as argument, a reference to the DatagramPacket object.	Invoke the receive method of the socket with a reference to the DatagramPacket object.

Fig. B.7.1 : Program flow in the sender and receiver process (adapted from [2])

a) Sending Process

- To send a datagram to another process, the sender process must instantiate a DatagramPacket object.
- DatagramPacket has information as given below :
  (1) Reference to a byte array which have all payload data
  (2) Destination address: It is combination of host ID and port number to which the receiver process DatagramSocket object is bound.

b) Receiving Process

- The receiving process must instantiate DatagramSocket object and bound to a local port
- This local port corresponds to the port number carried in the datagram packet of the sender.
- To receive datagrams sent to the socket, the receiving process must instantiate a DatagramPacket object that references a byte array and call the receive method of the DatagramSocket object, specifying as argument, a reference to the DatagramPacket object.

c) Process

- The program flow in the sender and receiver process is as shown in above Fig. B.7.1

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

3. Methods used in stream mode socket API

- The common key Methods of the Stream-Mode Socket API are explained as given below :

Sr. No.	Constructor/Method	Description
	DatagramSocket class	
1.	DatagramSocket( )	Create an object of class DatagramSocket Binds it to any available port on the local host machine.
2.	DatagramSocket(int port)	Create an object of class DatagramSocket Binds it to the specified port on the local host
3.	DatagramSocket (int port, InetAddressaddr)	Create an object of class DatagramSocket Binds it to the specified local address and port.
4.	void close( )	Closes the datagram socket
5.	void connect(InetAddress address, int port)	Connects the datagram socket to the specified remote address and port number on the machine with that address.
6.	InetAddress gerLocal Address( )	Returns the local InetAddress to which the socket is connected.
7.	int getLocalPort( )	Returns the port number on the local host to which the datagram socket is bound.
8.	InetAddress getInetAddress( )	Returns the IP address to which the datagram socket is connected to at the remote side.
9.	int getPort( )	Returns the port number at the remote side of the socket
10.	voidreceive (DatagramPacket packet)	Receives a datagram packet object from this socket
11.	void send(DatagraPacket packet)	Sends a datagram packet object from this socket.
12.	void setSoTimeout(int timeout)	Set the timeout value for the socket, in milliseconds

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Sr. No.	Constructor/Method	Description
	DatagramPacket class	
13.	DatagramPacket(byte[ ] buf, int length, InetAddress, int port)	Create a database packet object with the contents stored in a byte array, buffer of specified length to a machine with the specified IP address and port number
14.	InetAddress getAddress( )	Returns the IP address of the machine at the remote side to which the datagram is being sent or from which the datagram was received.
15.	byte [ ] getData( )	Returns the data buffer stored in the packet as a byte array.
16.	int getLength( )	Returns the length of the data buffer in the datagram packet sent or received.
17.	int getPort( )	Returns the port number to which the datagram socket is bound to which the datagram is being sent or from which the datagram is received
18.	void setData(byte [ ])	Sets the data buffer for the datagram packet
19.	void setAddress(InetAddress iaddr)	Sets the datagram packet with the IP address of the remote machine to which the packet is being sent.
20.	Void setPort(int port)	Sets the datagram packet with the port number of the datagram socket at the remote host to which the packet is sent.

4. Algorithm of UDP client socket programming

a) Find IP address and protocol number of host server

InetAddress receiverHost = InetAddress.getByName(args[0]);

int receiverPort = Integer.parseInt(args[1]);

b) Create a Socket Object

E.g. : DatagramSocket mySocket = new DatagramSocket( );

c) Specify that the connection needs an arbitrary, unused protocol port on local machine and allow UDP to select one and Specify the server to which messages must be sent.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

E.g.

```
DatagramPacket packet =
new DatagramPacket(buffer, buffer.length, receiverHost, receiverPort);
mySocket.send(packet);
```

d) Communicate with the server using application-level protocol

E.g.

```
mySocket.send(packet);
```

e) Close the socket

E.g.

```
mySocket.close( );
```

➢ **Program 2 : Connectionless (UDP) socket programming**

Code for Server:

```
import java.net.*;
import java.io.*;
class UDP_Server
{
public static void main(String[] args)
{
try{
System.out.println("-----------------------------------------");
    System.out.println("Program : UDP Server Socket");
    System.out.println("-----------------------------------------");
    InetAddress receiverHost = InetAddress.getByName(args[0]);
    int receiverPort = Integer.parseInt(args[1]);
    String message = args[2];
    DatagramSocket mySocket = new DatagramSocket( );
    byte[] buffer = message.getBytes( );
    DatagramPacket packet = new DatagramPacket(buffer, buffer.length, receiverHost,
    receiverPort);
    mySocket.send(packet);
    mySocket.close( );
  }
    catch(Exception e){ e.printStackTrace();}
    System.out.println("Message sent to client...");
    System.out.println("-----------------------------------------");
}
}
```

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Code for Client

```
import java.net.*;
import java.io.*;
class UDP_Client
{
public static void main(String[ ] args)
{
try{
    System.out.println("-----------------------------------------");
    System.out.println("Program : UDP Client Socket");
    System.out.println("-----------------------------------------");
    System.out.print("Message From Server is: ");
    int MAX_LEN = 40;
    int localPortNum = Integer.parseInt(args[0]);
    DatagramSocket mySocket = new DatagramSocket(localPortNum);
    byte[] buffer = new byte[MAX_LEN];
    DatagramPacket packet = new DatagramPacket(buffer, MAX_LEN);
    mySocket.receive(packet);
    String message = new String(buffer);
    System.out.println(message);
    System.out.println("-----------------------------------------");
    mySocket.close();
}
catch(Exception e){e.printStackTrace();}
}
}
```

Running above code :

Step 1 : Compile and run server socket

Copy java code file to bin folder of java

Compile UDP_Server.java program using javac command

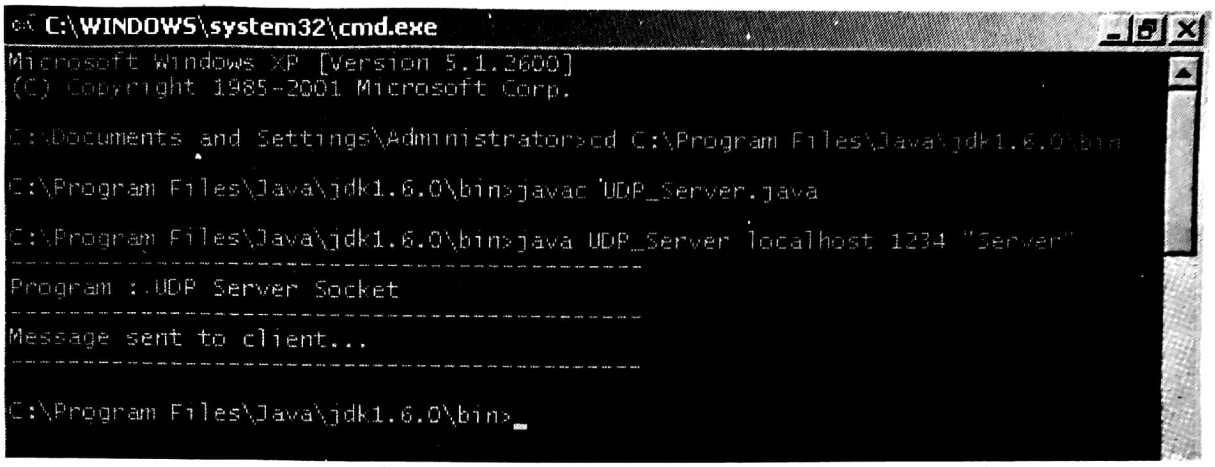
Run UDP_Server.java program using java command pass port number as argument in below program 1234 is port number.

Sever has sent message and do not wait for reply from client message so this message may loss if client is not receiving at that point of time.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Output :



Step 2: Compile and run Client socket

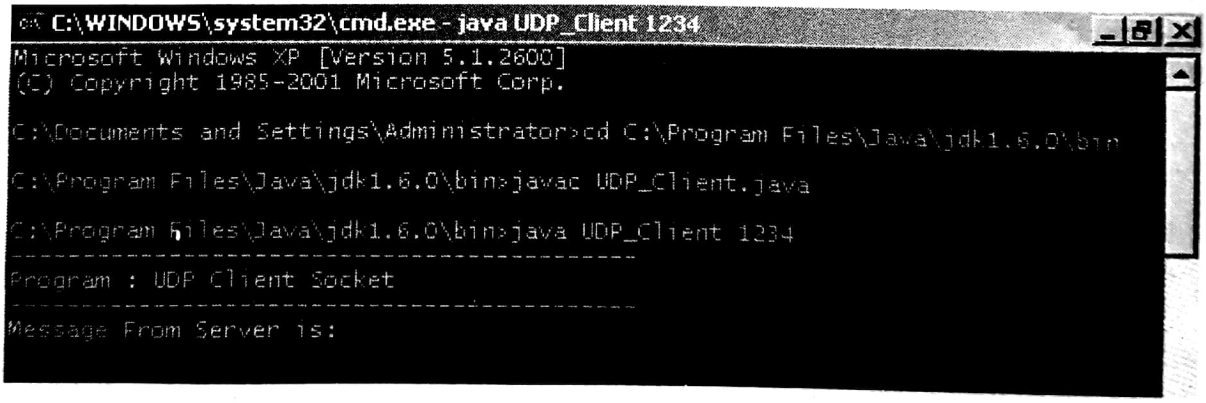
Copy java code file to bin folder of java

Compile UDP_Client.java program using javac command

Run UDP_Client.java program using java command pass port number as argument in below program 1234 is port number.

UDP_Client waiting for new message from server or sender.

Output :

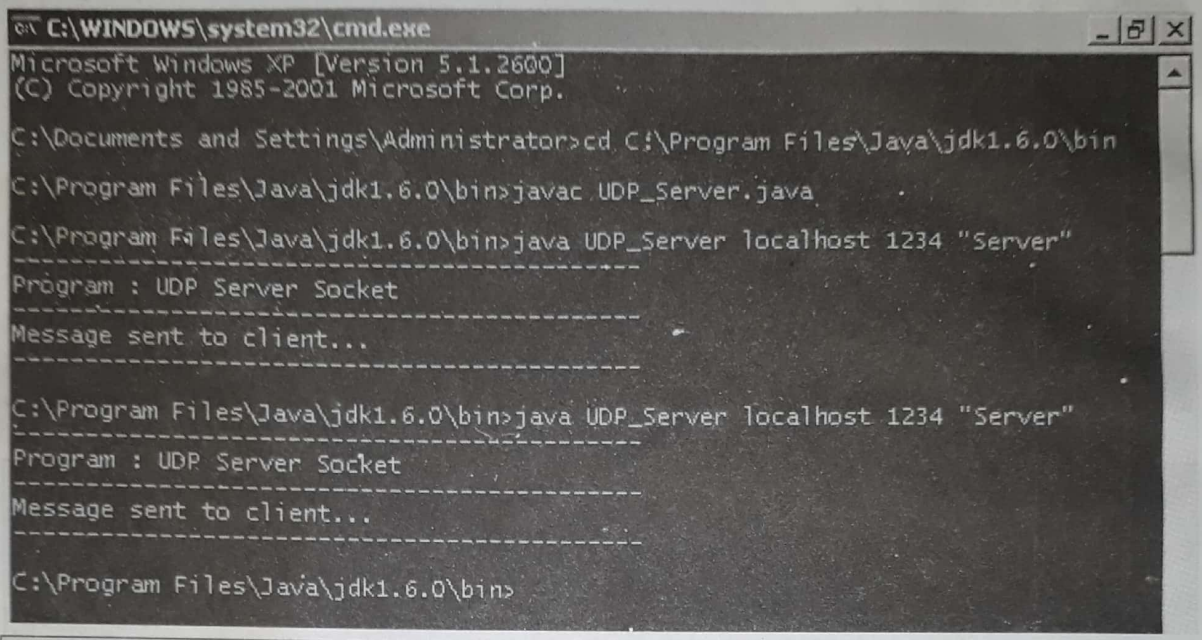


www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

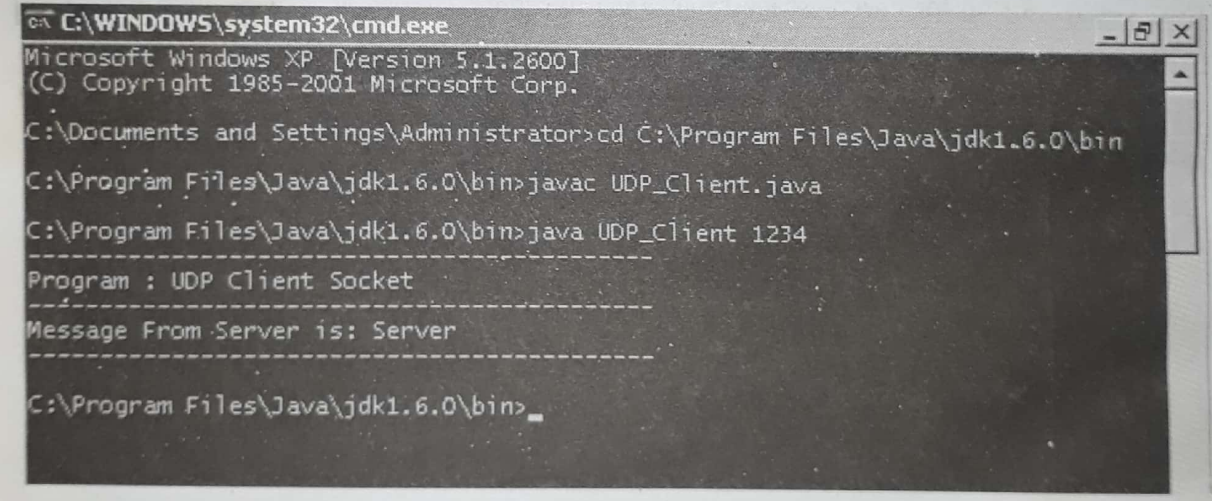
Step 3: Server socket Status after sending second message to client

Output :



Step 4 : Client socket has received message as it was now in listen mode

Output :



- In above example, DatagramSocket is a binding call. Once a datagram packet arrives at the receiver at the specified local port number where socket is opened and extract the bytes stored in the datagram packet to a string.
- Parameters are passed as :
  - The local port number known to the sender as well
  - Message to be sent

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

- The datagram sender (UDP_Server.java) program creates a DatagramPacket object and sets its destination IP address to the IP address of the remote host, the port number at which the message is expected to receive and the actual message.
- The sender program has nothing much to do after sending the message and hence the socket is closed.
- Similarly, the socket at the receiver side (UDP_Client) is also closed after receiving and printing the message.

B.8 Issues of Server

1. Introduction

- Server is a computer program that provides services to other computer programs in the same or other computers on network.
- Server socket application answers the client socket.
- There are number of clients connected with a single server so it faces many challenges while handling these client requests at a same point of time.

2. Concurrent vs iterative servers

- An iterative server is a server program which handles only one client program at any point of time.
- A concurrent server is a server program which can handle multiple client programs at any point of time.

3. Connection-oriented vs connection-less servers

- In a connection-oriented protocol, there is overhead of setting up a communications path between the sender and receiver, which will be maintained until the sender and receiver have completed their entire conversation.
- Connection-oriented protocols will provide guaranty of message delivery in the order in which they were sent.
- In a connectionless service, we do not require to establish a session or communication path.
- Connectionless services are like sending a postcard via post sender assumes that receiver will get it.

4. Stateful vs stateless servers

- A stateful server is a server program which maintains state of connected clients and their sessions in web servers.
- While stateless servers do not maintain state of connected clients and their sessions.

❑❑❑

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Note

www.MumbaiBScITStudy.Com

APRIL 2013

Q. 1 Answer any two of the following : **(10 Marks)**

(a) Show the unabbreviated colon hex notation for the following IPv6 addresses

i. An address with 64 0's followed by 64 1's.

ii. An address with 128 0's.

iii. An address with 128 1's.

iv. An address with 128 alternative 1's and 0's.

v. An address with two alternate 1's and 0's.

(b) Explain the use of time exceeded message of ICMP.

(c) Find the netid of the following IP addresses :

i) 114.34.2.8

ii) 132.56.8.6

iii) 208.34.54.12

iv) 251.34.98.5

v) 129.14.6.8

(d) Describe 3 phases of communication between remote host and mobiles host.

Q. 2 Answer any three of the following : **(15 Marks)**

(a) Describe the function of the transport layer in the OSI model.

(b) Explain the different kinds of classes along with their network mask for IPv4 addresses.

(c) List the component of IP packages ? Explain any one.

(d) Explain the transition strategies from IPv4 to IPv6.

(e) Find the error, if any, in the following IPv4 addresses :

i. 127.045.112.27

ii. 12.24.35.7.8

iii. 10110011.23.45.234

iv. 76.27.256.23

v. A23.56.78.5

(f) Differentiate between IPv4 and IPv6.

Mumbai B.Sc.IT Study

Q. 3 Answer any three of the following : (15 Marks)

(a) Explain the source quench message and time exceeded message in ICMPv4.

(b) What is the inefficiency in mobile IP? Give Solution for it.

(c) Explain the Input module of ARP.

(d) What are the three phases that a mobile host should go through to communicate with the remote host ?

(e) Explain the following terminologies related to OSPF protocol :

(i) Area (ii) Metric (iii) Link state database

(f) Explain path vector routing.

Q. 4 Answer any three of the following : (15 Marks)

(a) Explain Stop-and-wait Protocol and G0-Back-N Protocol in the transport layer.

(b) Explain the timers used in Transmission Control Protocol.

(c) Explain the features of Stream Control Transmission Protocol.

(d) List the multiple byte options supported by TCP. Explain any one with proper example.

(e) Explain the two-node loop problem of distance vector routing. Give the solution of it.

(f) A TCP connection is in ESTABLISHED. The following events occur one after another.

a. A FIN segment is received

b. The application sends a " close" message.

Q. 5 Answer any three of the following : (15 Marks)

(a) Explain the DHCP client transition diagram.

(b) What are the types of records used in Domain Name System?

(c) What is meant by resolution in DNS ? Explain.

(d) What are the types of TFTP messages? What is the purpose of each one?

(e) Define and give example of the following

i. Fully qualified domain name

ii. Partially qualified domain name

(f) List any five file management commands of FTP and write their purpose.

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Q. 6 Answer any three of the following : **(15 Marks)**

(a) Write a note on POP3.

(b) Explain the user agent component of electronic mail system.

(c) What are the types of Web documents?

(d) What is concept of SMI in SNMP?

(e) What are the different kinds of headers available in MIME?

(f) Write a short note on cookies.

□□□

www.MumbaiBScITStudy.Com

Mumbai B.Sc.IT Study

Note

www.MumbaiBScITStudy.Com

At Vidyalankar
Courses are Crafted to Deliver Fantastic Results

www.vidyalankar.org

B.Sc. (IT)

Race Ahead of others with our B. Sc. (IT) Coaching !

What our students say ...

Aggr. - 84.75%
T.Y.B.Sc. (IT)

Anagha Kotre

"Of the many advantages that Vidyalankar offers, three factors that equipped me really well for the exams were –their well-designed study material, comprising of notes, EQ (Examination Questions), GQ (Graded Questions), their distinct teaching methodology and their teachers, who are very, very helpful. They made sure that every single doubt we had was cleared and every problem on our mind solved."

DSS - 92/100

Archana Warrier

DSS - 90/100

Soniya Babwani

IT - 87/100

Mamata Jadhav

DW - 86/100

Amita Solanki

DW - 82/100

Neelam Anekar

IT - 82/100

Sandesh Patil

CMAT

Experience Vidyalankar's Unique Classroom Program
"MBA SMART CLASS PLUS" and Get into JBIMS or other Top B-Schools

What our students say ...

CMAT
99.54 Percentile

Ameya Gharpure

- I give full credit to Vidyalankar for successfully guiding me to achieve this result.
- Vidyalankar course Material has been specifically designed to meet the needs of all Aspirants. It takes care of the important concepts required for management entrance exams.

Admissions in Progress
To Enroll Call :
4232 4232

Be sure with
Vidyalankar®

Andheri	: 4232 14 00 / 2670 84 66	Borivali	: 4232 42 00 / 2891 05 21	Chembur	: 2528 31 62 / 2523 41 81
Dadar (E)	: 4232 12 00 / 2418 55 86	Dadar (W)	: 4232 42 32 / 2430 63 67	Dombivli	: 0251-248 03 21 / 28
Fort	: 2430 63 67	Ghatkopar	: 4232 24 00 / 2512 90 28	Nerul	: 2770 26 39 / 2770 26 42
Panvel	: 2745 99 66 / 2746 99 66	Thane	: 4232 22 00 / 2544 33 19	Vashi	: 4173 32 00 / 2789 31 85

Corporate Office :
Pearl Centre, Senapati Bapat Road, Dadar (West), Mumbai - 400 028.
Tel.: 4232 42 32 / 2430 63 67 • Fax : 2422 88 92
• www.vidyalankar.org

Books are available at :
KRISHNA BOOKS COLLECTIONS
Mahavir Market, Bhandarkar Road Matunga,
Central Railway Mumbai. Mob. 7498018909, 9820741455
Ph. : 022 (24099080)

ISBN : 978-93-5077-421-2

9 789350 774212

Price ₹ 165/-

SCAN TO VISIT
www.techmaxbooks.com

Tech-Max Publications

B/5, First Floor, Maniratna Complex, Aranyeshwar Corner,
Pune - 411009. Tel. : 91-20-24217965, 91-20-24225065
Fax : 020-24228978 Email : info@techmaxbooks.com

MU

INTERNET TECHNOLOGY

T. Y. B. Sc. (Information Technology) Semester - VI

Mahesh Mali
Chetana Khetmal

Book Code MIE21A
Price ₹ 165/-